

11.0 OfficeScan™

Manuel de l'administrateur

pour les grandes et moyennes entreprises



Endpoint Security



Protected Cloud



Web Security



Trend Micro Incorporated se réserve le droit de modifier sans préavis ce document et le produit décrit dans ce document. Avant d'installer et d'utiliser ce produit, veuillez consulter les fichiers Lisez-moi, les notes de mise à jour et/ou la version la plus récente de la documentation applicable, disponibles sur le site Web de Trend Micro à l'adresse suivante :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Nº de référence du document : OSEM115885_130313

Date de publication : avril 2014

Protégée par le brevet américain n° : 5,951,698

Cette documentation présente les principales fonctionnalités du produit et/ou fournit des instructions d'installation pour un environnement de production. Lisez attentivement cette documentation avant d'installer ou d'utiliser le produit.

Vous trouverez des informations détaillées sur l'utilisation des fonctions spécifiques du produit dans le centre d'aide en ligne et la Base de connaissances Trend Micro.

Trend Micro cherche toujours à améliorer sa documentation. Si vous avez des questions, des commentaires ou des suggestions à propos de ce document ou de tout autre document Trend Micro, veuillez nous contacter à l'adresse docs@trendmicro.com.

Vous pouvez évaluer cette documentation sur le site Web suivant :

http://www.trendmicro.com/download/documentation/rating.asp



Table des matières

Préface

Partie I: Introduction et guide de démarrage

Chapitre 1: Présentation d'OfficeScan

Chapitre 2: Démarrage d'OfficeScan

Chapitre 3: Démarrage de la protection des données

Partie II: Protection des agents OfficeScan

Chapitre 4: Utilisation de Trend Micro Smart Protection

Chapitre 5: Installation de l'agent OfficeScan

Chapitre 6: Maintien d'une protection à jour

Chapitre 7: Recherche des risques de sécurité

Chapitre 8: Utilisation de la surveillance des comportements

Chapitre 9: Utilisation du contrôle des dispositifs

Chapitre 10: Utilisation de la prévention contre la perte de données

Chapitre 11: Protection des ordinateurs contre les menaces Internet

Chapitre 12: Utilisation du pare-feu OfficeScan

Partie III: Gestion du serveur et des agents OfficeScan

Chapitre 13: Gestion du serveur OfficeScan

Chapitre 15: Utilisation de Plug-in Manager

Chapitre 16: Ressources de dépannage

Chapitre 17: Assistance technique

Annexes

Annexe A: Prise en charge de l'adressage IPv6 dans OfficeScan

Annexe B: Prise en charge de Windows Server Core 2008/2012

Annexe C: Prise en charge de Windows 8/8.1 et Windows Server 2012

Annexe D: Rétrogradation d'OfficeScan

Annexe E: glossaire

Index



Préface

Préface

Bienvenue dans le *Manuel de l'administrateur* de Trend Micro™OfficeScan™. Ce document fournit des informations relatives au démarrage, ainsi que les procédures d'installation des agents, et aborde l'administration des serveurs et des agents OfficeScan.

Les rubriques sont les suivantes :

Documentation OfficeScan

La documentation OfficeScan comprend les documents suivants :

TABLEAU 1. Documentation OfficeScan

DOCUMENTATION	DESCRIPTION
Guide d'installation et de mise à niveau	Document PDF qui aborde les éléments requis et les procédures d'installation du serveur OfficeScan, ainsi que les informations nécessaires pour la mise à niveau du serveur et des agents.
Manuel de l'administrateur	Document PDF contenant des informations relatives au démarrage, ainsi que les procédures d'installation des agents, et abordant l'administration des serveurs et des agents OfficeScan.
Aide	Fichiers HTML compilés au format WebHelp ou CHM contenant des descriptions de procédures, des conseils d'utilisation et des informations relatives aux champs. L'Aide est accessible depuis les consoles du serveur et de l'agent OfficeScan, ainsi que depuis le programme principal d'installation d'OfficeScan.
Fichier Lisez-moi	contient une liste des problèmes connus et les étapes d'installation de base. Il peut aussi contenir des informations relatives au produit qui n'ont pas pu être intégrées à temps dans l'aide ou dans la documentation imprimée
Base de connaissances	Base de données en ligne contenant des informations sur la résolution des problèmes et le dépannage. Elle contient les dernières informations sur les problèmes connus identifiés pour les produits. Pour accéder à la base de connaissances, consultez le site Web suivant : http://esupport.trendmicro.com

Téléchargez les versions les plus récentes des documents PDF et du fichier Lisez-moi à l'adresse :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Public cible

La documentation OfficeScan est destinée aux catégories d'utilisateurs suivantes :

- **AdministrateursOfficeScan** : responsables de l'administration d'OfficeScan, ce qui inclut l'installation et la gestion des serveurs et des agents OfficeScan. Ces utilisateurs sont supposés posséder des connaissances approfondies dans le domaine de la gestion des réseaux et des serveurs.
- **Utilisateurs finaux** : utilisateurs sur les ordinateurs desquels est installé l'agent OfficeScan. Leur niveau de compétence en informatique va du débutant à l'expert.

Conventions typographiques du document

Pour faciliter la recherche et la compréhension des informations, la documentation OfficeScan utilise les conventions suivantes :

Tableau 2. Conventions typographiques du document

Nomenclature	Description
MAJUSCULES	Acronymes, abréviations, noms de certaines commandes et touches sur le clavier
Gras	Menus et commandes de menus, boutons de commande, onglets, options et tâches
Italique	Références à d'autres documents ou nouveaux composants technologiques
Agents > **Gestion des agents**	« Chemin de navigation » indiqué au début des procédures qui aide les utilisateurs à naviguer vers l'écran approprié de la console Web. La présence de plusieurs chemins de navigation indique qu'il existe plusieurs façons d'accéder à un même écran.
<Texte>	Indique que le texte entre crochets doit être remplacé par les données elles-mêmes. Par exemple, `C:\Program Files\<nom_fichier>` peut correspondre à `C:\Program Files\sample.jpg`.

NOMENCLATURE	DESCRIPTION
Remarque	Fournit des recommandations ou des remarques de configuration
Conseil	Informe sur les pratiques recommandées et les recommandations de Trend Micro
AVERTISSEMENT!	Procure des avertissements sur les activités susceptibles de nuire aux ordinateurs de votre réseau

Terminologie

Le tableau ci-dessous présente la terminologie officielle employée dans toute la documentation OfficeScan :

TABLEAU 3. Terminologie OfficeScan

TERMINOLOGIE	DESCRIPTION
Agent OfficeScan	Programme de l'agent OfficeScan
Endpoint de l'agent	Endpoint sur lequel l'agent OfficeScan est installé
Utilisateur de l'agent (ou utilisateur)	Personne qui gère l'agent OfficeScan sur le endpoint de l'agent
Serveur	Programme serveur OfficeScan
Ordinateur serveur	Endpoint sur lequel le serveur OfficeScan est installé.
Administrateur (ou administrateur OfficeScan)	Personne qui gère le serveur OfficeScan

TERMINOLOGIE	DESCRIPTION
Console	Interface utilisateur permettant de configurer et de gérer les paramètres des serveurs et des agents OfficeScan. La console employée pour le programme du serveur OfficeScan est appelée « console Web » et celle employée pour le programme de l'agent OfficeScan est appelée « console de l'agent ».
Risque liés à la sécurité	Terme générique regroupant les virus/programmes malveillants, les spywares/graywares et les menaces Internet
Service licence	Inclut les services antivirus, Damage Cleanup Services, les services de réputation de sites Web et anti-spyware, qui sont tous activés lors de l'installation du serveur OfficeScan
Service OfficeScan	Services hébergés via Microsoft Management Console (MMC). Par exemple, `ofcservice.exe`, le service principal d'OfficeScan.
Programme	Inclut l'agent OfficeScan et Plug-in Manager.
Composants	Responsables du scan, de la détection et des actions contre les risques liés à la sécurité

`Dossier d'installation de l'agent`	Dossier du endpoint qui contient les fichiers de l'agent OfficeScan. Si vous acceptez les paramètres par défaut pendant l'installation, vous trouverez le dossier d'installation à l'un des emplacements suivants :
	
	`C:\Program Files\Trend Micro\OfficeScan Client`
	
	`C:\Program Files (x86)\Trend Micro\OfficeScan Client`

TERMINOLOGIE	DESCRIPTION

`Dossier d'installation du serveur`	Dossier du endpoint qui contient les fichiers du serveur OfficeScan. Si vous acceptez les paramètres par défaut pendant l'installation, vous trouverez le dossier d'installation à l'un des emplacements suivants :
	`C:\Program Files\Trend Micro\OfficeScan`
	`C:\Program Files (x86)\Trend Micro\OfficeScan`
	Par exemple, si un fichier particulier se trouve dans `\PCCSRV` du dossier d'installation du serveur, le chemin d'accès complet au fichier est le suivant :
	`C:\Program Files\Trend Micro\OfficeScan\PCCSRV\<file_name>.`

Agent Smart Scan	Agent OfficeScan ayant été configuré pour utiliser Smart Scan.
Agent de scan traditionnel	Agent OfficeScan ayant été configuré pour utiliser le scan traditionnel.
Double pile	Entités ayant à la fois une adresse IPv4 et une adresse IPv6. Par exemple : • Endpoints ayant à la fois une adresse IPv4 et une adresse IPv6. • Agents OfficeScan installés sur des endpoints à double pile. • Agents de mise à jour chargés de distribuer les mises à jour aux autres agents. • Serveur proxy à double pile, tel que DeleGate, pouvant effectuer la conversion entre adresses IPv4 et IPv6.
IPv4 pur	Une entité n'ayant qu'une adresse IPv4
IPv6 pur	Une entité n'ayant qu'une adresse IPv6

TERMINOLOGIE	DESCRIPTION
Solutions de plug-in	Fonctions natives d'OfficeScan et modules additionnels proposés via Plug-in Manager.

Partie I

Introduction et guide de démarrage



Chapitre 1

Présentation d'OfficeScan

Ce chapitre présente Trend Micro™OfficeScan™ et offre un aperçu de ses fonctions et fonctionnalités.

Les rubriques sont les suivantes :

À propos d'OfficeScan

Trend Micro™ OfficeScan™ protège les réseaux d'entreprise contre les programmes malveillants, les virus de réseau, les menaces provenant d'Internet, les spywares et les menaces combinées. Solution intégrée, OfficeScan est composé du programme de l'agent OfficeScan, qui réside sur le endpoint, et d'un programme serveur, qui gère tous les agents. L'agent OfficeScan protège le endpoint et communique au serveur son état de sécurité. Le serveur, via une console d'administration à interface Web, facilite l'application coordonnée de stratégies de sécurité et le déploiement de mises à jour vers chaque agent.

OfficeScan fonctionne sous Trend Micro Smart Protection Network™, une infrastructure de contenu client en ligne de nouvelle génération qui offre une sécurité plus intelligente que celle des méthodes classiques. Une technologie en ligne unique et l'allégement de l'agent réduisent le besoin de téléchargements conventionnels de fichiers de signatures et éliminent les retards couramment associés aux mises à jour des postes de travail. Les entreprises bénéficient d'une augmentation de la bande passante réseau, d'une réduction de la puissance de traitement et d'une diminution des coûts générés. Les utilisateurs accèdent immédiatement à la protection la plus récente où qu'ils se connectent, du réseau de l'entreprise, de leur domicile ou en déplacement.

Nouveautés de cette version

Trend Micro OfficeScan inclut les nouvelles fonctionnalités et améliorations suivantes.

Nouveautés d'OfficeScan 11.0

Cette version d'OfficeScan inclut les nouvelles fonctions et améliorations suivantes :

Tableau 1-1. Améliorations apportées au serveur

Fonction	Description
Outil de migration de base de données SQL	Les administrateurs peuvent choisir de migrer la base de données serveur CodeBase® existante vers une base de données SQL Server. Pour obtenir des informations détaillées, consultez la section *Outil de migration SQL Server à la page 13-45*.
Amélioration apportées au serveur Smart Protection Server	Cette version d'OfficeScan prend en charge la version mise à niveau du serveur Smart Protection Server 3.0. La version mise à niveau du serveur Smart Protection Server inclut des améliorations apportées aux fichiers de signatures des services File Reputation. Les fichiers de signatures ont été remodelés afin de fournir les avantages suivants : • Réduction de la consommation de mémoire • Mises à jour incrémentielle des fichiers de signatures et détection améliorée des fichiers de signatures des services File Reputation, ce qui réduit de manière significative la consommation de bande passante
Authentification serveur	Des clés d'authentification serveur améliorées permettent à toutes les communications entrantes et sortantes du serveur d'être sécurisées et fiables. Pour obtenir des informations détaillées, consultez la section *Authentification des communications provenant du serveur à la page 13-51*.
Améliorations apportées à l'administration basée sur les rôles	Les améliorations apportées à l'administration basée sur les rôles fluidifient la façon dont les administrateurs configurent les rôles et les comptes, ce qui simplifie l'intégration avec Trend Micro Control Manager™. Pour obtenir des informations détaillées, consultez la section *Administration basée sur les rôles à la page 13-2*.
Configuration du serveur Web	Cette version d'OfficeScan peut être intégrée à un serveur Web Apache 2.2.25.

Fonction	Description
Nouvelle conception de l'interface du serveur OfficeScan	L'interface OfficeScan a été remodelée afin de fournir une expérience simplifiée et plus moderne. Toutes les fonctionnalités disponibles dans la version précédente du serveur OfficeScan le sont toujours dans cette version mise à jour. • Options de menu de niveau supérieur pour libérer de l'espace sur l'écran. • Menu « Favoris » pour vous permettre d'accéder aux écrans que vous utilisez souvent. • Affichage en diaporama des onglets du **Tableau de bord** permettant de consulter les données des widgets sans avoir à contrôler manuellement la console.
Aide en ligne contextuelle	L'aide en ligne contextuelle est mise à jour en permanence et permet aux administrateurs d'avoir toujours accès aux informations les plus récentes. Si aucune connexion Internet n'est disponible, OfficeScan passe automatiquement au système d'aide local fourni avec le produit.
Plates-formes et navigateurs pris en charge	OfficeScan prend en charge les systèmes d'exploitation suivants : • Windows Server™ 2012 R2 (serveur et agent) • Windows 8.1 (agent uniquement) OfficeScan prend en charge le navigateur suivant : • Internet Explorer™ 11.0

Tableau 1-2. Améliorations apportées aux agents

Fonction	Description
Restauration depuis la mise en quarantaine centrale	OfficeScan permet aux administrateurs de restaurer des fichiers « suspects » précédemment détectés et d'ajouter des fichiers aux listes d'éléments « approuvés » au niveau du domaine afin d'empêcher l'exécution de toute action sur ces fichiers. Si un programme ou un fichier a été détecté ou mis en quarantaine, les administrateurs peuvent restaurer ces fichiers sur les agents de manière globale ou individuelle. Les administrateurs peuvent faire appel à une vérification SHA1 supplémentaire afin de s'assurer que les fichiers qu'ils souhaitent restaurer n'ont subi aucune modification. Une fois les fichiers restaurés, OfficeScan peut automatiquement les ajouter aux listes des exclusions au niveau du domaine afin de leur épargner tout scan futur. Pour obtenir des informations détaillées, consultez la section *Restauration de fichiers mis en quarantaine à la page 7-46*.
Service de protection avancé	Le service de protection avancé fournit les nouvelles fonctionnalités de scan suivantes : • La prévention contre l'exploitation du navigateur utilise une technologie de bac à sable pour tester le comportement de pages Web en temps réel et détecter tout script ou programme malveillant avant même que l'agent OfficeScan ne soit exposé à des menaces. Pour obtenir des informations détaillées, consultez la section *Configuration de Stratégie de réputation de sites Web à la page 11-6*. • Le scan amélioré de la mémoire, allié à la surveillance des comportements, peut détecter des variantes de programmes malveillants lors des scans en temps réel et prendre les actions nécessaires (mise en quarantaine) contre les menaces. Pour obtenir des informations détaillées, consultez la section *Paramètres de scan à la page 7-29*.

Fonction	Description
Améliorations apportées à la protection des données	La protection des données OfficeScan a été améliorée afin de fournir les avantages suivants : • Découverte des données via une intégration avec Control Manager™ : les administrateurs peuvent configurer des stratégies de prévention contre la perte de données sur Control Manager afin de scanner les dossiers des agents OfficeScan à la recherche de fichiers contenant des données sensibles. Lorsque des données sensibles ont été découvertes dans un fichier, Control Manager peut consigner l'emplacement du fichier ou, grâce à l'intégration avec Trend Micro Endpoint Encryption, chiffrer automatiquement le fichier sur l'agent OfficeScan. • Prise en charge de la fonction de justification de l'utilisateur : les administrateurs peuvent permettre aux utilisateurs de fournir un motif lors du transfert de données sensibles ou bloquer eux-mêmes les transmissions. OfficeScan consigne toutes les tentatives de transfert ainsi que les motifs fournis par l'utilisateur. Pour obtenir des informations détaillées, consultez la section *Mesures de prévention contre la perte de données à la page 10-38*. • Prise en charge pour smartphones et tablettes : la prévention contre la perte de données et le contrôle des dispositifs peuvent désormais surveiller les données sensibles envoyées sur des appareils mobiles et prendre les actions nécessaires les concernant, ou encore bloquer complètement tout envoi vers de tels appareils. Pour obtenir des informations détaillées, consultez la section *Contrôle des dispositifs à la page 9-2*. • Bibliothèques d'identificateurs de données et de modèles mises à jour : les bibliothèques de prévention contre la perte de données ont été mises à jour et contiennent désormais 2 nouvelles listes de mots-clés et 93 nouveaux modèles. • Intégration des journaux de contrôle des dispositifs avec Control Manager™

Fonction	Description
Améliorations apportées aux paramètres de connexion suspecte	Les services d'alerte de contact C&C (Command & Control) ont été mis à jour afin d'inclure ce qui suit : • Listes globales des adresses IP approuvées et bloquées définies par l'utilisateur. Pour obtenir des informations détaillées, consultez la section *Configuration des paramètres des listes globales des adresses IP définies par l'utilisateur à la page 11-14*. • Utilisation du système de reconnaissance réseau des programmes malveillants pour détecter les rappels C&C. • Configuration d'actions détaillées lors de la détection de connexions suspectes. Pour obtenir des informations détaillées, consultez la section *Configuration des paramètres de connexion suspecte à la page 11-15*. • Consignation dans les journaux C&C des serveurs et des agents des processus responsables des rappels C&C
Améliorations apportées à la prévention des épidémies	La prévention des épidémies a été mise à jour afin d'assurer une protection contre les éléments suivants : • Fichiers compressés exécutables Pour obtenir des informations détaillées, consultez la section *Refus de l'accès aux fichiers compressés exécutables à la page 7-118*. • Processus Mutex. Pour obtenir des informations détaillées, consultez la section *Création d'une règle de traitement par exclusion mutuelle pour les fichiers/processus de programmes malveillants à la page 7-117*.

Fonction	Description
Améliorations apportées aux fonctionnalités d'autoprotection	Les fonctionnalités d'autoprotection disponibles dans cette version fournissent des solutions à la fois peu invasives et hautement sécurisées afin de protéger les programmes de votre serveur et de l'agent OfficeScan. • Solution peu invasive : conçue pour les plates-formes serveur afin de protéger le processus et les clés de Registre de l'agent OfficeScan par défaut, sans toutefois affecter les performances du serveur. • Solution hautement sécurisée : améliore la fonctionnalité d'autoprotection de l'agent disponible dans les versions précédentes en fournissant les éléments suivants : • Authentification des commandes IPC. • Protection et vérification des fichiers de signatures. • Protection des mises à jour des fichiers de signatures. • Protection du processus de surveillance des comportements. Pour obtenir des informations détaillées, consultez la section *Autoprotection de l'agent OfficeScan à la page 14-13*.

FONCTION	DESCRIPTION
Améliorations apportées aux performances et à la détection des scans	• Le scan en temps réel dispose d'une mémoire cache persistante rechargée à chaque démarrage de l'agent OfficeScan. Si des fichiers ou des dossiers ont été modifiés depuis le dernier déchargement de l'agent OfficeScan, ce dernier les supprime de la mémoire cache. • Cette version d'OfficeScan inclut des listes globales d'éléments approuvés pour les fichiers système Windows, les fichiers signés numériquement provenant de sources fiables, ainsi que les fichiers testés par Trend Micro. S'il s'avère qu'un fichier est sans danger, OfficeScan n'exécute aucune action dessus. • Les améliorations apportées à Damage Cleanup Services ont un impact positif sur les fonctionnalités de détection pour les menaces liées aux rootkits et diminuent le nombre de faux positifs grâce à un scan GeneriClean mis à jour. • Les paramètres des fichiers compressés sont distincts pour les scans en temps réel et les scans à la demande, afin d'améliorer les performances. Pour obtenir des informations détaillées, consultez la section *Configurer les paramètres de scan pour les gros fichiers compressés à la page 7-75*. • Des journaux à double couche fournissent un aperçu plus détaillé des détections dont les administrateurs souhaiteraient approfondir l'examen.
Nouvelle conception de l'interface de l'agent OfficeScan	L'interface de l'agent OfficeScan a été remodelée afin de fournir une expérience simplifiée et plus moderne. Toutes les fonctionnalités disponibles dans la version précédente du programme client OfficeScan le sont toujours dans cette version mise à jour. L'interface mise à jour permet également aux administrateurs de « déverrouiller » des fonctions d'administration directement depuis la console de l'agent OfficeScan afin de pouvoir régler rapidement les problèmes sans avoir à ouvrir la console Web.

Fonctionnalités et avantages principaux

OfficeScan fournit les fonctionnalités et avantages suivants :

- **Plug-In Manager et solutions modules additionnels**

  Plug-in Manager facilite l'installation, le déploiement et la gestion des solutions modules additionnels.

  Les administrateurs peuvent installer deux types de solutions de plug-in :

  - Programmes plug-in
  - Fonctions natives d'OfficeScan

- **Gestion centralisée**

  Une console d'administration à interface Web offre aux administrateurs un accès transparent à tous les agents et serveurs du réseau. La console Web coordonne le déploiement automatique des stratégies de sécurité, des fichiers de signatures et des mises à jour logicielles sur chaque agent et chaque serveur. De plus, grâce à Outbreak Prevention Services, les vecteurs d'infection sont bloqués et les stratégies de sécurité spécifiques aux attaques sont rapidement déployées pour prévenir ou contenir les épidémies avant que les fichiers de signatures ne soient disponibles. OfficeScan effectue également une surveillance en temps réel, avec notification d'événements et génération de rapports complets. Les administrateurs peuvent effectuer des tâches d'administration à distance, définir des stratégies personnalisées pour des postes de travail individuels ou des groupes et verrouiller les paramètres de sécurité des agents.

- **Protection contre les risques de sécurité**

  OfficeScan protège les ordinateurs contre les risques de sécurité en scannant les fichiers avant de mener une action spécifique selon chaque risque détecté. Un nombre élevé de risques de sécurité détectés en peu de temps témoigne d'une épidémie. Pour enrayer les épidémies, OfficeScan applique des stratégies de prévention des épidémies et isole les ordinateurs sur lesquels sont détectés les fichiers infectés jusqu'à ce qu'ils ne présentent plus aucun risque.

  OfficeScan utilise Smart Scan pour optimiser l'efficacité du processus de scan. Cette technologie consiste à transférer un nombre important de signatures

précédemment stockées sur le endpoint local vers des sources Smart Protection. Cette démarche réduit considérablement l'impact sur les systèmes et sur le réseau du volume sans cesse croissant de mises à jour de signatures vers les endpoints.

Pour plus d'informations concernant Smart Scan et son déploiement sur les agents, voir *Types de méthodes de scan à la page 7-9*.

- **Damage Cleanup Services**

  Damage Cleanup Services™ débarrasse les ordinateurs des virus basés sur fichiers et des virus de réseau, ainsi que des résidus de virus et de vers (chevaux de Troie, entrées de Registre, fichiers viraux) et ce, à l'aide d'un processus totalement automatisé. Pour traiter les menaces et les nuisances générées par les chevaux de Troie, Damage Cleanup Services effectue les actions suivantes :

  - Détecte et supprime les chevaux de Troie actifs
  - Élimine les processus créés par les chevaux de Troie
  - Répare les fichiers système modifiés par les chevaux de Troie
  - Supprime les fichiers et les applications laissés par les chevaux de Troie

  Les services Damage Cleanup Services s'exécutent automatiquement en arrière-plan ; vous n'avez donc pas besoin de les configurer. Les utilisateurs ne remarquent même pas son activité. Toutefois, OfficeScan peut parfois demander à l'utilisateur de redémarrer son endpoint pour terminer le processus de suppression d'un cheval de Troie.

- **Réputation de sites Web**

  La technologie de réputation de sites Web protège de manière proactive les ordinateurs des agents au sein du réseau d'entreprise ou en-dehors de celui-ci contre les sites Web malveillants et potentiellement dangereux. La réputation de sites Web rompt la chaîne d'infection et empêche le téléchargement de code malveillant.

  Vérifiez la crédibilité des sites et des pages Web en intégrant OfficeScan au serveur Smart Protection Server ou à Trend Micro Smart Protection Network.

- **Pare-feu OfficeScan**

  Le pare-feu OfficeScan protège les agents et les serveurs du réseau grâce à une fonction « Stateful inspection » et à des scans antivirus de réseau hautes

performances. Créez des règles pour filtrer les connexions par application, adresse IP, numéro de port ou protocole, puis appliquez-les à différents groupes d'utilisateurs.

- **Prévention contre la perte de données**

  La prévention contre la perte de données protège les actifs numériques d'une entreprise contre les fuites de données, délibérées ou accidentelles. La prévention contre la perte des données permet aux administrateurs ce qui suit :

  - L'identification de l'actif numérique à protéger
  - La création de stratégies qui limitent ou empêchent la transmission d'actifs numériques par les canaux de transmission classiques, tels que les e-mails et les dispositifs externes.
  - Le renforcement de la conformité à des normes de confidentialité établies

- **Contrôle des dispositifs**

  Le Contrôle des dispositifs régule l'accès aux périphériques de stockage externes et ressources réseau connectés aux ordinateurs. Le Contrôle des dispositifs prévient la perte et les fuites de données et, conjointement avec le scan de fichiers, contribue à la protection contre les risques de sécurité.

- **Surveillance des comportements**

  La surveillance des comportements contrôle en continu les agents, guettant des modifications inhabituelles apportées au système d'exploitation ou aux logiciels installés.

Le serveur OfficeScan

Le serveur OfficeScan est un référentiel central contenant l'ensemble des configurations des agents, des journaux de risques de sécurité et des mises à jour.

Le serveur exécute deux tâches primordiales :

- Il installe, surveille et gère les agents OfficeScan.

- Il télécharge la plupart des composants dont les agents ont besoin. Le serveur OfficeScan télécharge les composants depuis le serveur ActiveUpdate de Trend Micro, puis les distribue aux agents.



Remarque

Certains composants sont téléchargés par les sources Smart Protection. Voir *Sources Smart Protection à la page 4-6* pour obtenir des informations détaillées.



FIGURE 1-1. Fonctionnement du serveur OfficeScan

Le serveur OfficeScan est capable d'établir une communication bidirectionnelle en temps réel entre le serveur et les agents OfficeScan. Vous pouvez gérer les agents depuis

une console Web basée sur navigateur à laquelle les administrateurs peuvent accéder depuis la quasi-totalité du réseau. Le serveur communique avec l'agent (et l'agent avec le serveur) via le protocole HTTP (HyperText Transfer Protocol).

L'agent OfficeScan

Vous pouvez protéger les ordinateurs Windows contre les risques de sécurité en installant l'agent OfficeScan sur chaque endpoint.

L'agent OfficeScan dépend du serveur parent à partir duquel il a été installé. Vous pouvez configurer les agents pour qu'ils dépendent d'un autre serveur à l'aide de l'outil Agent Mover. L'agent envoie en temps réel au serveur des informations relatives à son état et à des événements. Les événements transmis sont notamment la détection d'un virus/programme malveillant, le démarrage d'un agent, la déconnexion d'un agent, le lancement d'un scan et la réalisation d'une mise à jour.

Intégration aux produits et services de Trend Micro

OfficeScan s'intègre aux produits et services Trend Micro mentionnés dans le tableau suivant. Pour une intégration sans difficulté, assurez-vous que les produits fonctionnent avec les versions requises ou recommandées.

Tableau 1-3. Produits et services qui s'intègrent à OfficeScan

Produit/ Service	Description	Version
Serveur ActiveUpdate	Fournit tous les composants nécessaires à l'agent OfficeScan pour protéger les agents des menaces de sécurité.	Non applicable
Smart Protection Network	Fournit aux agents des services File Reputation et des services de réputation de sites Web. Smart Protection Network est hébergé par Trend Micro.	Non applicable

Produit/ Service	Description	Version
Serveur Smart Protection Server autonome	Fournit les mêmes services de File Reputation et de réputation de sites Web que Smart Protection Network. Un serveur autonome Smart Protection Server est destiné à localiser le service sur le réseau de l'entreprise afin d'assurer une efficacité optimale. **Remarque** Un serveur Smart Protection Server intégré est installé sur le serveur OfficeScan Server. Il possède les mêmes fonctions que le serveur autonome, mais ses capacités sont limitées.	• 3.0
Control Manager	Solution de gestion logicielle vous permettant de contrôler l'antivirus et les programmes de sécurisation du contenu depuis un emplacement central, indépendamment de la plate-forme ou de l'emplacement physique du programme.	• 6.0 SP1 (recommandé) • 6.0 • 5.5 SP1
Deep Discovery Advisor	Deep Discovery fournit une surveillance du réseau en s'appuyant sur l'analyse sandbox personnalisée et sur les renseignements utiles collectés en temps réel. Il détecte et bloque rapidement les attaques et fournit des mises à jour de sécurité personnalisées améliorant instantanément la protection contre de futures attaques.	3.0 et version ultérieure



Chapitre 2

Démarrage d'OfficeScan

Ce chapitre décrit comment démarrer avec Trend Micro™OfficeScan™ et les paramètres de configuration initiaux.

Les rubriques sont les suivantes :

La console Web

La console Web est le point central permettant de surveiller sur l'ensemble du réseau de l'entreprise. La console présente des paramètres et des valeurs par défaut que vous pouvez configurer en fonction de vos spécifications et exigences de sécurité. La console Web utilise des technologies Internet standard telles que Java, CGI, HTML et HTTPS.



Remarque

Configurez les paramètres de délai d'attente depuis la console Web. Voir la section *Paramètres de la console Web à la page 13-56*.

Utilisez la console Web pour effectuer les opérations suivantes :

- Gérer les agents installés sur des ordinateurs en réseau
- Regrouper des agents par domaines logiques pour permettre de les configurer et de les gérer tous ensemble
- Définir des configurations de scan et lancer un scan manuel sur un ou plusieurs ordinateurs en réseau
- Configurer des notifications liées aux risques de sécurité affectant le réseau et afficher les journaux envoyés par les agents
- Configurer les critères et les notifications d'épidémie
- Déléguer des tâches d'administration de la console Web à d'autres administrateurs OfficeScan en configurant les rôles et les comptes utilisateurs
- S'assurer que les agents respectent les consignes de sécurité



Remarque

La console Web ne prend pas en charge Windows 8, 8.1 ni Windows Server 2012 en mode Windows UI.

Configuration requise pour l'ouverture de la console Web

Ouvrez la console Web depuis tout endpoint du réseau disposant des ressources suivantes :

- Processeur Intel™ Pentium™ 300MHz ou équivalent
- 128 Mo de mémoire vive
- Au moins 30 Mo d'espace disque disponible
- Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum
- Microsoft Internet Explorer™ 8.0 ou ultérieur



Remarque

OfficeScan prend uniquement en charge le trafic HTTPS pour l'affichage de la console Web.

Sur le navigateur Web, entrez l'une des adresses suivantes dans la barre d'adresses en fonction du type d'installation du serveur OfficeScan :

Tableau 2-1. URL de la console Web d'OfficeScan

Type d'installation	URL
Sans SSL sur un site par défaut	https://<Nom de domaine complet ou adresse IP du serveur OfficeScan>/OfficeScan
Sans SSL sur un site virtuel	https://<Nom de domaine complet ou adresse IP du serveur OfficeScan>:<numéro de port HTTP>/OfficeScan
Avec SSL sur un site par défaut	https://<Nom de domaine complet ou adresse IP du serveur OfficeScan>/OfficeScan

TYPE D'INSTALLATION	URL
Avec SSL sur un site virtuel	`https://<Nom de domaine complet ou adresse IP du serveur OfficeScan>/OfficeScan`

Remarque

Si vous avez procédé à une mise à niveau à partir d'une version antérieure OfficeScan, les fichiers de mémoire cache du serveur proxy et du navigateur Web peuvent empêcher le chargement correct de la console Web d'OfficeScan. Videz la mémoire cache du navigateur et celle de tout serveur proxy situé entre le serveur OfficeScan et le endpoint que vous utilisez pour accéder à la console Web.

Compte de connexion

Pendant l'installation du serveur OfficeScan, le programme d'installation crée un compte racine et vous invite à saisir le mot de passe de ce compte. Lors de la première ouverture de la console Web, saisissez «racine» comme nom d'utilisateur et mot de passe de compte racine. Si vous avez oublié votre mot de passe, contactez votre service d'assistance pour qu'il vous aide à le réinitialiser.

Définissez des rôles utilisateurs et configurez les comptes utilisateurs de façon à permettre à d'autres utilisateurs d'accéder à la console Web sans employer le compte racine. Lorsqu'ils se connectent, les utilisateurs peuvent se servir des comptes utilisateurs que vous avez configurés pour eux. Pour plus d'informations, voir *Administration basée sur les rôles à la page 13-2*.

La bannière de la console Web

Dans la zone de la bannière de la console Web, vous disposez des options suivantes :

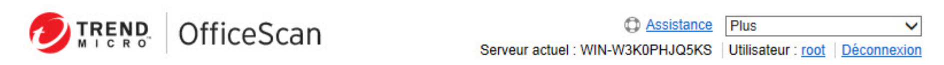


FIGURE 2-1. Zone bannière de la console Web

- **Assistance technique** : affiche la page Web d'assistance technique de Trend Micro, sur laquelle vous pouvez poser des questions et trouver des réponses aux questions les plus fréquentes concernant les produits Trend Micro.
- **Plus**
    - **Encyclopédie des menaces** : affiche le site Web de l'encyclopédie des menaces, qui renferme toutes les informations liées aux programmes malveillants dont Trend Micro dispose. Les experts en menaces de Trend Micro publient régulièrement leurs trouvailles en matière de détection de programmes malveillants, spam, URL malveillantes et vulnérabilités. L'encyclopédie des menaces explique également le déroulement des attaques Web les plus courantes et fournit des informations connexes.
    - **Rechercher un distributeur** : affiche la page **Nous contacter** du site Web de Trend Micro, qui contient les coordonnées de nos bureaux dans le monde entier.
    - **À propos de** : fournit une vue d'ensemble du produit, des instructions pour vérifier les détails des versions de composants et un lien vers Assistance Intelligence System. Pour obtenir des informations détaillées, voir *Assistance Intelligence System à la page 16-2*.
- **<nom du compte>** : cliquez sur le nom du compte (par exemple, racine) pour changer des informations du compte (par exemple, le mot de passe).
- **Déconnexion** : déconnecte l'utilisateur de la console Web

Le Tableau de bord

Le **Tableau de bord** s'affiche lorsque vous ouvrez la console Web OfficeScan ou cliquez sur **Tableau de bord** dans le menu principal.

Chaque compte utilisateur de la console Web dispose d'un tableau de bord totalement indépendant. Aucun changement dans les paramètres de tableau de bord d'un compte utilisateur n'affectera les tableaux de bord des autres comptes utilisateurs.

Si un tableau de bord contient les données d'un agent OfficeScan, les données qui s'affichent dépendent des autorisations du compte utilisateur sur le domaine de l'agent.

Par exemple, si vous accordez à un compte utilisateur les autorisations nécessaires pour gérer les domaines A et B, le tableau de bord du compte utilisateur n'affichera que les données des agents appartenant aux domaines A et B.

Pour obtenir des détails sur les comptes utilisateurs, voir *Administration basée sur les rôles à la page 13-2*.

L'écran **Tableau de bord** comprend les éléments suivants :

- Section de l'état de la licence de produit
- Widgets
- Onglets

Section de l'état de la licence de produit

Cette section se situe au-dessus du tableau de bord et affiche l'état des licences OfficeScan.

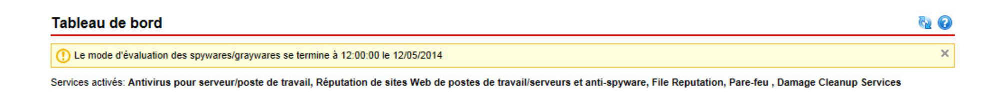


FIGURE 2-2. Section de l'état de la licence de produit

Des messages de rappel concernant l'état de la licence s'affichent dans les cas suivants :

- Si vous possédez une licence de version complète :
    - 60 jours avant l'expiration d'une licence
    - Pendant la période de grâce du produit. La durée de la période de grâce varie selon les régions. Veuillez vérifier cette durée auprès de votre représentant Trend Micro.
    - Une fois la licence expirée et la période de grâce écoulée: pendant cette période, vous ne pourrez ni obtenir d'assistance technique ni effectuer de mises à jour des composants. Les moteurs de scan continueront à scanner les

ordinateurs à l'aide des composants obsolètes. Ces composants obsolètes ne peuvent pas vous protéger entièrement contre les derniers risques de sécurité.

- Si vous possédez une licence de version d'évaluation :
  - 14 jours avant l'expiration d'une licence
  - Une fois la licence expirée: Pendant cette période, OfficeScan désactive les mises à jour des composants, les scans, ainsi que toutes les fonctionnalités des agents.

Si vous avez obtenu un code d'activation, renouvelez votre licence en accédant à **Administration** > **Paramètres** > **Licence du produit**.

Barres d'informations sur le produit

OfficeScan affiche divers messages dans la partie supérieure de l'écran **Tableau de bord**, afin de fournir des informations supplémentaires aux administrateurs.

Les informations affichées sont notamment :

- Les Service Packs ou patches les plus récents disponibles pour OfficeScan.



Remarque

Cliquez sur **Informations supplémentaires** pour télécharger le patch depuis le centre de téléchargement de Trend Micro (http://downloadcenter.trendmicro.com/?regs=FR).

- Les nouveaux widgets disponibles.
- Des notifications relatives au certificat d'authentification en cas d'expiration du certificat en cours ou lorsqu'aucune sauvegarde n'existe.
- Des notifications relatives au contrat de maintenance lorsque celui-ci est sur le point d'expirer.
- Des notifications relatives au mode d'évaluation.
- Des notifications relatives à l'authenticité des produits.



Remarque

Si la licence utilisée pour OfficeScan n'est pas authentique, un message d'information s'affiche. Si vous ne faites pas l'acquisition d'une licence authentique, OfficeScan affiche un avertissement et ne procède plus à aucune mise à jour.

Onglets et widgets

Les widgets constituent les composants centraux du tableau de bord. Les widgets fournissent des informations spécifiques sur les différents événements liés à la sécurité. Certains widgets vous permettent d'exécuter certaines tâches, telles que la mise à jour de vieux composants.

Les informations fournies par les widgets proviennent des sources suivantes :

- serveur et agents OfficeScan
- solutions modules additionnels et leurs agents
- Trend Micro Smart Protection Network



Remarque

Activez Smart Feedback afin d'afficher les données de Smart Protection Network. Pour plus d'informations sur Smart Feedback, voir *Smart Feedback à la page 13-61*.

Les onglets fournissent un endroit pour accueillir les widgets. Le **Tableau de bord** peut contenir un maximum de 30 onglets.

Utilisation des onglets

Gérez les onglets en exécutant les tâches suivantes :

TABLEAU 2-2. Tâches via les onglets

<table>
<tr><th>TÂCHE</th><th>ÉTAPES</th></tr>
<tr><td>Ajouter un nouvel onglet</td><td>1. Cliquez sur l'icône Ajouter situé au-dessus du tableau de bord. Un nouvel écran s'affiche.
OfficeScan | OfficeScan et les plug-ins | Smart Protection Network | +
2. Indiquez ce qui suit :
• Titre : le nom de l'onglet
• Disposition : choisissez parmi les dispositions disponibles
• Ajustement automatique : Activez l'ajustement automatique si vous avez choisi une disposition avec plusieurs zones (telle que « ») et que chaque zone ne comportera qu'un seul widget. L'ajustement automatique ajuste les widgets afin qu'ils rentrent dans la zone.
3. Cliquez sur Enregistrer.</td></tr>
<tr><td>Modifier les paramètres d'onglets</td><td>1. Cliquez sur Paramètres d'onglets dans l'angle droit de l'onglet. Un nouvel écran s'affiche.
Paramètres des onglets
2. Modifiez le nom de l'onglet, sa disposition et ses paramètres d'ajustement automatique.
3. Cliquez sur Enregistrer.</td></tr>
<tr><td>Déplacer un onglet</td><td>Utilisez le glisser-déplacer pour déplacer un onglet.</td></tr>
<tr><td>Supprimer un onglet</td><td>Cliquez sur l'icône Supprimer située à côté du titre de l'onglet.
Smart Scan Agents ✕
La suppression d'un onglet supprime également tous les widgets de l'onglet.</td></tr>
</table>

Utilisation des widgets

Gérez les widgets en exécutant les tâches suivantes :

TABLEAU 2-3. Tâches des widgets

TÂCHE	ÉTAPES
Faire défiler les onglets	Cliquez sur **Faire défiler les onglets** pour passer automatiquement de l'affichage d'un onglet à un autre.
Ajouter un nouveau widget	1. Cliquez sur un onglet. 2. Cliquez sur **Ajouter des widgets** dans l'angle supérieur droit de l'onglet. Un nouvel écran s'affiche. 3. Sélectionnez les widgets à ajouter. Pour une liste des widgets disponibles, voir *Widgets disponibles à la page 2-12*. • Cliquez sur les icônes d'affichage ( ) en haut à droite de l'écran afin de basculer entre l'affichage Détaillé et l'affichage Résumé. • À gauche de l'écran se trouvent les catégories de widgets. Sélectionnez une catégorie afin d'affiner les sélections. • Utilisez la zone de recherche de texte située en haut de l'écran afin de rechercher un widget spécifique. 4. Cliquez sur **Ajouter**.
Déplacer un widget	Faites glisser les widgets pour les déplacer vers une zone différente au sein de l'onglet.
Redimensionner un widget	Redimensionnez un widget dans un onglet à plusieurs colonnes en pointant le curseur sur la bordure droite du widget, puis en déplaçant le curseur vers la gauche ou la droite.

Tâche	Étapes
Modifier le titre du widget	1. Cliquez sur l'icône Modifier ( ). Un nouvel écran s'affiche. 2. Saisissez le nouveau titre. **Remarque** Pour certains widgets, tels que le Mashup d'OfficeScan et des plug-ins, des éléments liés aux widgets peuvent être modifiés. 3. Cliquez sur **Enregistrer**.
Rafraîchir les données du widget	Cliquez sur l'icône Actualiser ( ).
Supprimer un widget	Cliquez sur l'icône Supprimer ( ).

Onglets et widgets prédéfinis

Le **Tableau de bord** est fourni avec un ensemble d'onglets et de widgets prédéfinis. Vous pouvez renommer ou supprimer ces onglets et widgets.

Tableau 2-4. Onglets par défaut du Tableau de bord

Onglet	Description	Widgets
OfficeScan	Cet onglet contient les mêmes informations que celles de l'écran **Tableau de bord** des versions précédentes d'OfficeScan. Dans cet onglet, vous pouvez avoir un aperçu de la protection contre les risques liés à la sécurité du réseau OfficeScan. Vous pouvez également agir sur les éléments nécessitant une intervention immédiate, tels que les épidémies ou les composants obsolètes.	• *Widget Connectivité de l'agent antivirus à la page 2-15* • *Widget de détection des risques liés à la sécurité à la page 2-20* • *Widget Épidémies à la page 2-20* • *Widget Mises à jour de l'agent à la page 2-22*

ONGLET	DESCRIPTION	WIDGETS
OfficeScan et les plug-ins	Cet onglet présente les agents OfficeScan et les solutions modules additionnels en cours d'exécution sur les agents. Utilisez cet onglet pour évaluer l'état de sécurité général des agents.	*Widget Mashup d'OfficeScan et des modules additionnels à la page 2-23*
Smart Protection Network	Cet onglet contient des informations provenant de Trend Micro Smart Protection Network, qui fournit des services File Reputation et de réputation de sites Web aux agents OfficeScan.	• *Widget Sources majeures des menaces selon la réputation des sites Web à la page 2-30* • *Widget Utilisateurs les plus menacés selon la réputation des sites Web à la page 2-31* • *Widget Carte des menaces de File Reputation à la page 2-32*

Widgets disponibles

Les widgets suivants sont disponibles dans cette version :

TABLEAU 2-5. Widgets disponibles

NOM DU WIDGET	DISPONIBILITÉ
Connectivité de l'agent antivirus	Disponible et prêt à l'emploi Pour obtenir des informations détaillées, voir *Widget Connectivité de l'agent antivirus à la page 2-15*.
Détection des risques liés à la sécurité	Disponible et prêt à l'emploi Pour obtenir des informations détaillées, voir *Widget de détection des risques liés à la sécurité à la page 2-20*.

Nom du widget	Disponibilité
Épidémies	Disponible et prêt à l'emploi Pour obtenir des informations détaillées, voir *Widget Épidémies à la page 2-20*.
Mises à jour de l'agent	Disponible et prêt à l'emploi Pour obtenir des informations détaillées, voir *Widget Mises à jour de l'agent à la page 2-22*.
Mashup d'OfficeScan et des modules additionnels	Disponible et prêt à l'emploi mais n'affiche que les données des agents OfficeScan Les données des solutions de plug-in suivantes sont disponibles après avoir activé chaque solution : • Intrusion Defense Firewall • Trend Micro Virtual Desktop Support Pour obtenir des informations détaillées, voir *Widget Mashup d'OfficeScan et des modules additionnels à la page 2-23*.
Incidents majeurs de prévention contre la perte de données	Disponible après avoir activé la protection des données OfficeScan Pour obtenir des informations détaillées, voir *Widget Incidents majeurs de prévention contre la perte de données à la page 2-25*.
Incidents de prévention contre la perte de données dans le temps	Disponible après avoir activé la protection des données OfficeScan Pour obtenir des informations détaillées, voir *Widget Incidents de prévention contre la perte de données dans le temps à la page 2-26*.
Sources majeures des menaces selon la réputation des sites Web	Disponible et prêt à l'emploi Pour obtenir des informations détaillées, voir *Widget Sources majeures des menaces selon la réputation des sites Web à la page 2-30*.

Nom du widget	Disponibilité
Utilisateurs les plus menacés selon la réputation des sites Web	Disponible et prêt à l'emploi Pour obtenir des informations détaillées, voir *Widget Utilisateurs les plus menacés selon la réputation des sites Web à la page 2-31*.
Carte des menaces de File Reputation	Disponible et prêt à l'emploi Pour obtenir des informations détaillées, voir *Widget Carte des menaces de File Reputation à la page 2-32*.
Événements de rappel C&C	Disponible et prêt à l'emploi Pour obtenir des informations détaillées, voir *Widget Événements de rappel C&C à la page 2-28*.
IDF - État d'alerte	Disponible après avoir activé Intrusion Defense Firewall. Pour plus d'informations concernant ces widgets, voir la documentation IDF.
IDF - État de l'ordinateur	
IDF - Historique des événements du réseau	
IDF - Historique des événements du système	

Widget Connectivité agent-serveur

Le widget **Connectivité agent-serveur** affiche l'état de la connexion de tous les agents avec le serveur OfficeScan. Les données s'affichent dans un tableau et un graphique

circulaire. Vous pouvez basculer entre le tableau et le graphique circulaire en cliquant sur les icônes d'affichage ( ).

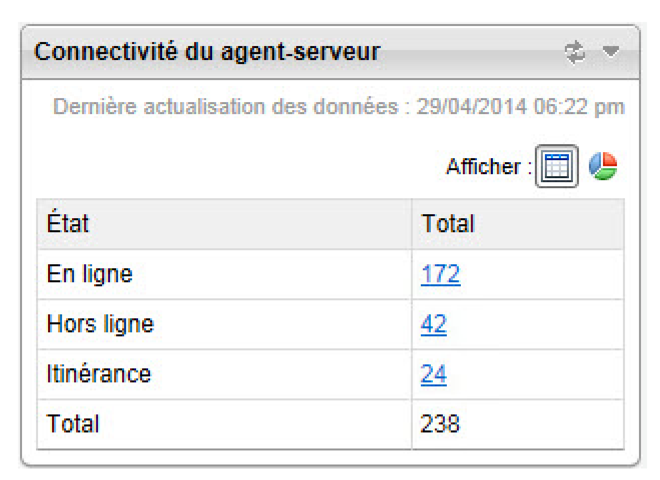


FIGURE 2-3. Widget Connectivité agent-serveur affichant un tableau

Widget Connectivité de l'agent antivirus

Le widget **Connectivité de l'agent antivirus** affiche l'état de la connexion des agents antivirus avec le serveur OfficeScan. Les données s'affichent dans un tableau et un

graphique circulaire. Vous pouvez basculer entre le tableau et le graphique circulaire en cliquant sur les icônes d'affichage ().

Connectivité de l'agent antivirus

Dernière actualisation des données : 06/05/2014 06:02 pm

Tout

Afficher :

État	Smart Scan	Scan traditionnel	Total
En ligne	86	86	172
Hors ligne	21	21	42
Itinérance	12	12	24
Total	119	119	238

FIGURE 2-4. Widget Connectivité de l'agent antivirus affichant un tableau

Widget Connectivité de l'agent antivirus sous forme de tableau

Le tableau distingue les agents par méthodes de scan.

Si le nombre d'agents pour un état particulier est supérieur ou égal à 1, vous pouvez cliquer sur le chiffre afin d'afficher ces agents dans l'arborescence des agents. Vous pouvez exécuter des tâches sur ces agents ou modifier leurs paramètres.

Pour afficher uniquement les agents utilisant une méthode de scan particulière, cliquez sur **Tous**, puis sélectionnez la méthode de scan.

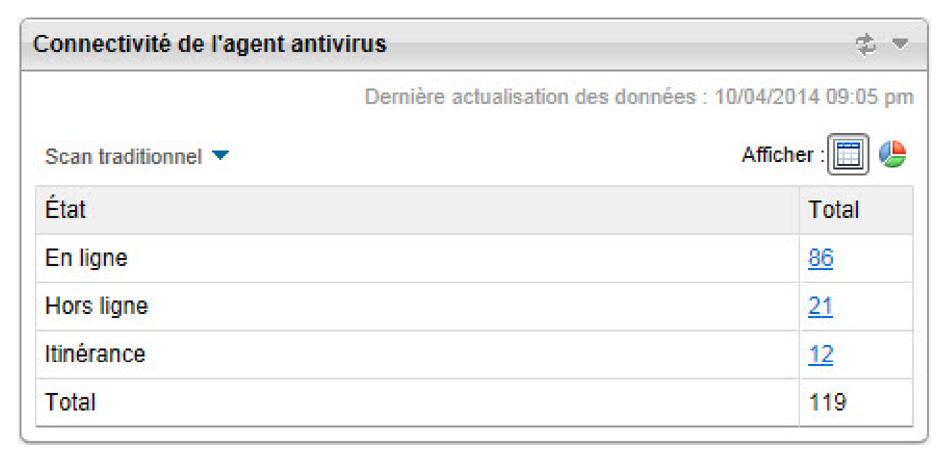


FIGURE 2-5. État de la connexion des agents de scan traditionnel

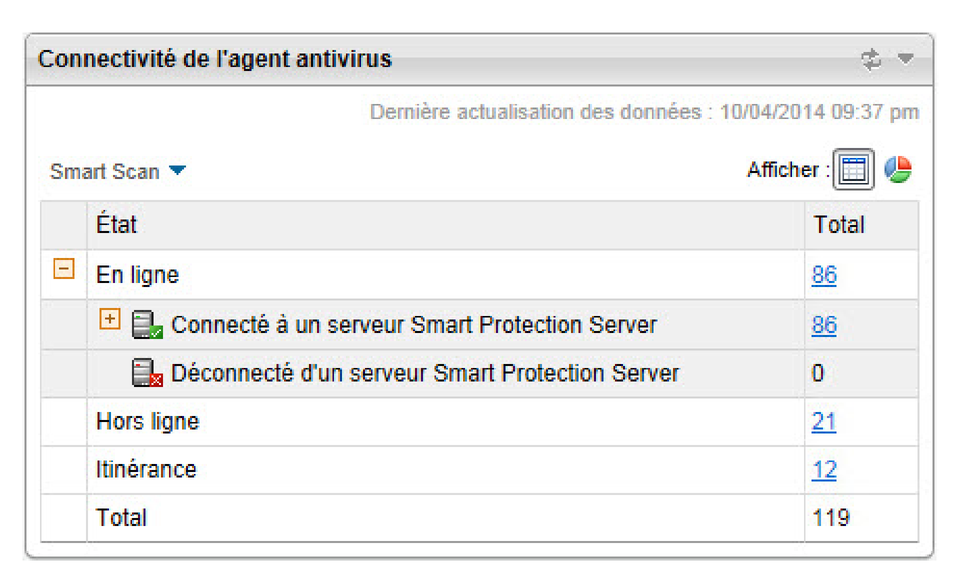


FIGURE 2-6. État de la connexion des agents Smart Scan

Si vous avez sélectionné **Smart Scan** :

- Le tableau distingue les agents Smart Scan en ligne en fonction de l'état de leur connexion aux serveurs Smart Protection Server.



Remarque

Seuls les agents en ligne peuvent signaler leur état de connexion aux serveurs Smart Protection Server.

Si des agents sont déconnectés d'un serveur Smart Protection Server, restaurez la connexion en suivant les étapes indiquées à la rubrique *Solutions aux problèmes indiqués par les icônes de l'agent OfficeScan à la page 14-41*.

- Chaque serveur Smart Protection Server possède une URL sur laquelle cliquer pour lancer la console du serveur.
- S'il y a plusieurs serveurs Smart Protection Server, cliquez sur **PLUS**. Un nouvel écran s'ouvre, affichant tous les serveurs Smart Protection Server.

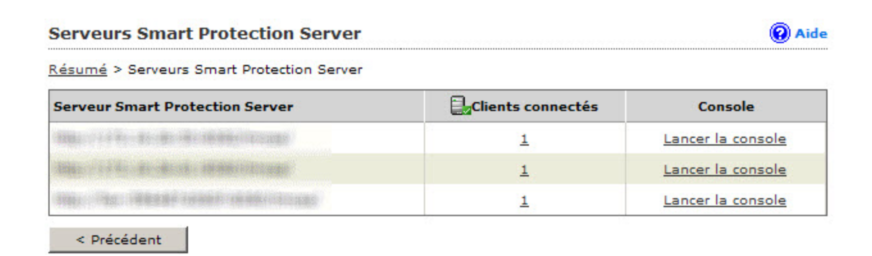


FIGURE 2-7. Liste Serveurs Smart Protection Server

Dans cet écran, vous pouvez :

- Afficher tous les serveurs Smart Protection Server auxquels les agents sont connectés, ainsi que le nombre d'agents connectés à chaque serveur. Un clic sur le chiffre permet d'ouvrir l'arborescence des agents, depuis laquelle vous pouvez gérer les paramètres des agents.

- Lancer une console de serveur en cliquant sur le lien menant au serveur

Widget Connectivité de l'agent antivirus sous forme de graphique circulaire

Le graphique circulaire affiche uniquement le nombre d'agents pour chaque état et ne distingue pas les agents en fonction des méthodes de scan. Cliquer sur un statut permet de le séparer ou de le reconnecter au reste du graphique.

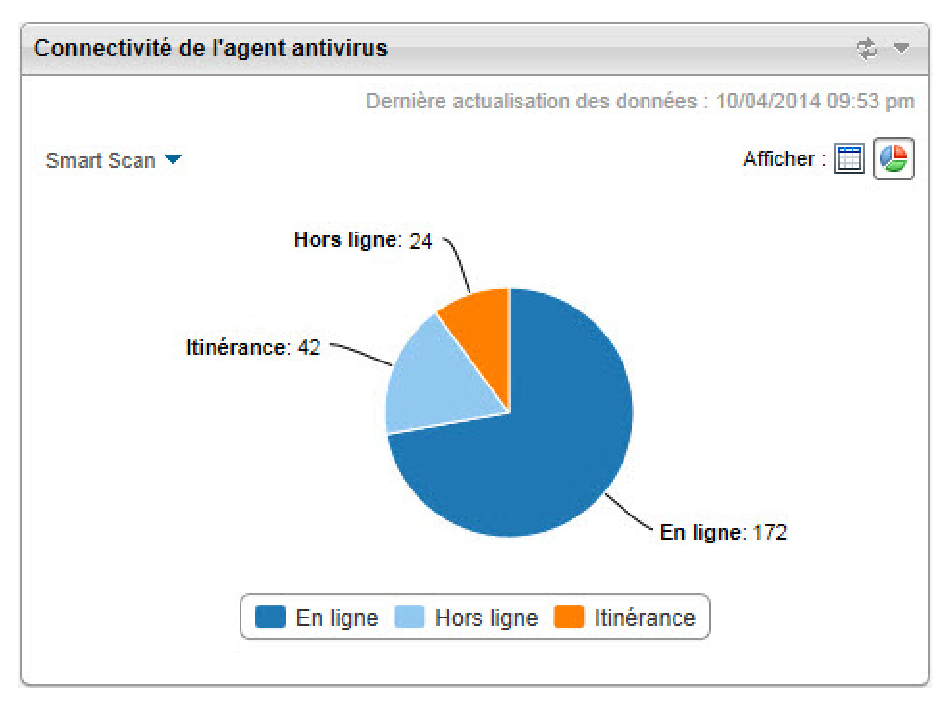


FIGURE 2-8. Widget Connectivité de l'agent antivirus affichant un graphique circulaire

Widget de détection des risques liés à la sécurité

Le widget **Détection des risques de sécurité** affiche le nombre de risques de sécurité et de endpoints infectés.



FIGURE 2-9. Widget de détection des risques liés à la sécurité

Si le nombre de endpoints infectés est supérieur ou égal à 1, vous pouvez cliquer sur le chiffre afin d'afficher les endpoints infectés dans l'arborescence des agents. Vous pouvez lancer des tâches sur les agents OfficeScan résidant sur ces endpoints ou modifier leurs paramètres.

Widget Épidémies

Le widget **Épidémies** affiche l'état de toute épidémie de risque de sécurité actuelle, ainsi que la dernière alerte d'épidémie.

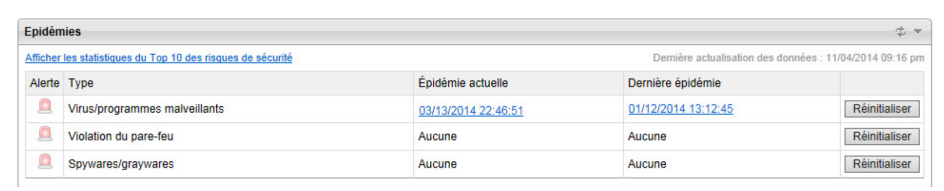


FIGURE 2-10. Widget Épidémies

Dans ce widget, vous pouvez effectuer les actions suivantes :

- Consultez les informations détaillées sur une épidémie en cliquant le lien Date/ Heure de l'alerte.
- Dès qu'OfficeScan détecte une épidémie, réinitialisez l'état des informations d'alerte d'épidémie et appliquez immédiatement les mesures de prévention d'épidémie. Pour plus d'informations sur l'application des mesures de prévention des épidémies, voir *Stratégies de prévention des épidémies à la page 7-112*.
- Cliquez sur **Afficher les statistiques du Top 10 des risques de sécurité** afin d'afficher les risques liés à la sécurité les plus courants, les ordinateurs comptant le plus grand nombre de risques et les sources d'infections principales. Un nouvel écran s'affiche.

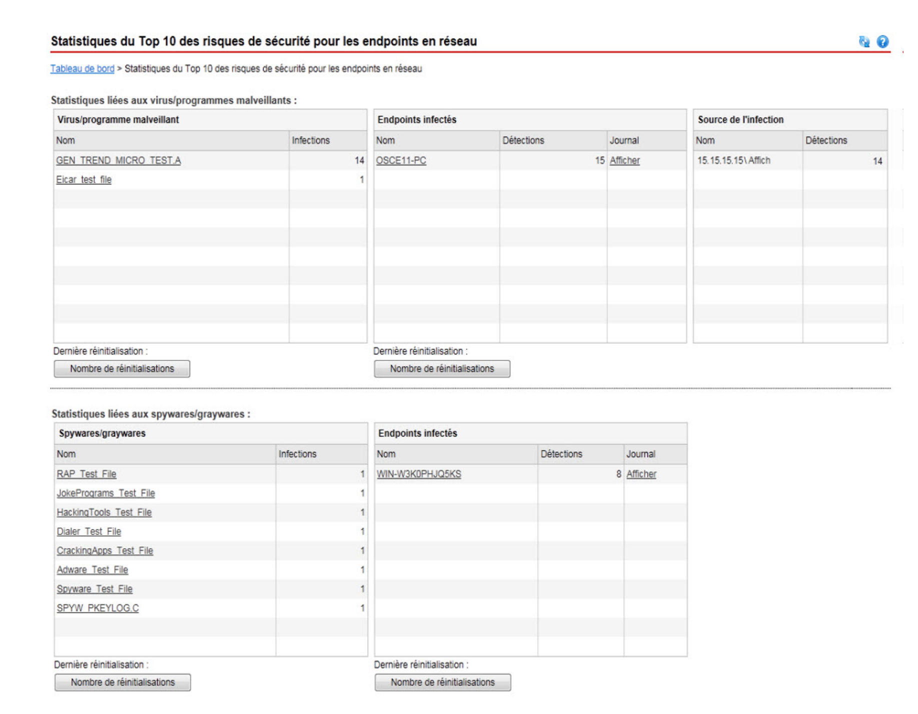


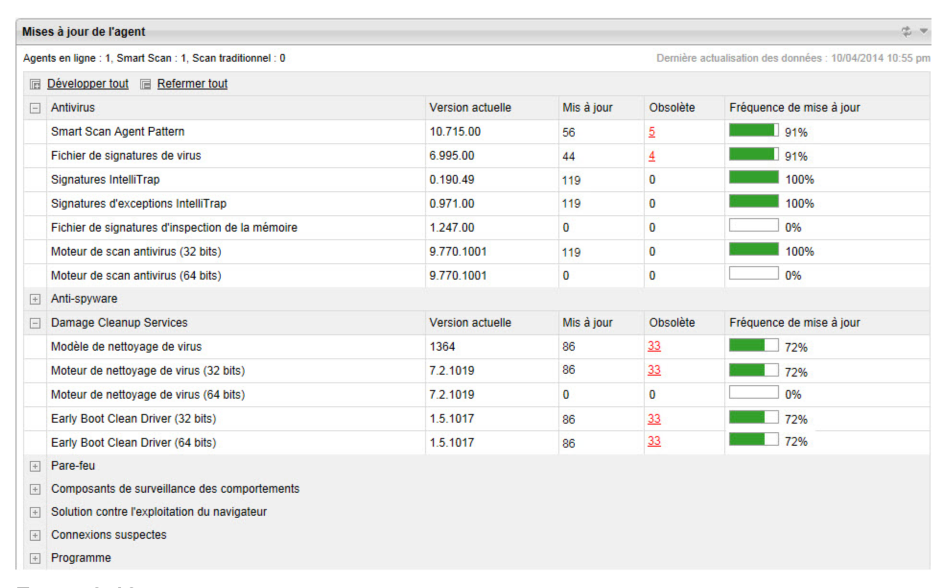
FIGURE 2-11. Écran Statistiques du Top 10 des risques de sécurité pour les endpoints en réseau

Sur l'écran des **statistiques du Top 10 des risques de sécurité**, vous pouvez :

- Consulter des informations détaillées sur un risque de sécurité en cliquant sur le nom de ce risque.
- Consulter l'état général d'un endpoint particulier en cliquant sur son nom.
- Consulter les journaux de risques de sécurité relatifs à ce endpoint en cliquant sur le bouton **Afficher** correspondant au nom de ce endpoint.
- Réinitialiser les statistiques dans chaque tableau en cliquant sur **Réinitialiser nombre**.

Widget Mises à jour de l'agent

Le widget **Mises à jour de l'agent** affiche les composants et programmes protégeant vos endpoints en réseau des risques de sécurité.



Mises à jour de l'agent

Agents en ligne : 1, Smart Scan : 1, Scan traditionnel : 0 — Dernière actualisation des données : 10/04/2014 10:55 pm

Développer tout — Refermer tout

Antivirus	Version actuelle	Mis à jour	Obsolète	Fréquence de mise à jour
Smart Scan Agent Pattern	10.715.00	56	5	91%
Fichier de signatures de virus	6.995.00	44	4	91%
Signatures IntelliTrap	0.190.49	119	0	100%
Signatures d'exceptions IntelliTrap	0.971.00	119	0	100%
Fichier de signatures d'inspection de la mémoire	1.247.00	0	0	0%
Moteur de scan antivirus (32 bits)	9.770.1001	119	0	100%
Moteur de scan antivirus (64 bits)	9.770.1001	0	0	0%
Anti-spyware				
Damage Cleanup Services	Version actuelle	Mis à jour	Obsolète	Fréquence de mise à jour
Modèle de nettoyage de virus	1364	86	33	72%
Moteur de nettoyage de virus (32 bits)	7.2.1019	86	33	72%
Moteur de nettoyage de virus (64 bits)	7.2.1019	0	0	0%
Early Boot Clean Driver (32 bits)	1.5.1017	86	33	72%
Early Boot Clean Driver (64 bits)	1.5.1017	86	33	72%
Pare-feu				
Composants de surveillance des comportements				
Solution contre l'exploitation du navigateur				
Connexions suspectes				
Programme				

FIGURE 2-12. Widget Mises à jour de l'agent

Dans ce widget, vous pouvez effectuer les actions suivantes :

- Affichez la version actuelle de chaque composant.
- Sous la colonne **Obsolète**, affichez le nombre d'agents dont les composants sont obsolètes. Si certains agents ont besoin d'être mis à jour, cliquez sur le lien numéroté pour démarrer cette mise à jour.
- Pour chaque programme, vous pouvez afficher les agents n'ayant pas été mis à niveau en cliquant sur le lien numéroté correspondant au programme.

Widget Mashup d'OfficeScan et des modules additionnels

Le widget **Mashup d'OfficeScan et des modules additionnels** combine les données des agents OfficeScan et des modules additionnels installés, puis les présente dans l'arborescence des agents. Ce widget vous aide à évaluer rapidement le niveau de protection des agents et réduit le temps nécessaire à la gestion de chaque module additionnel.

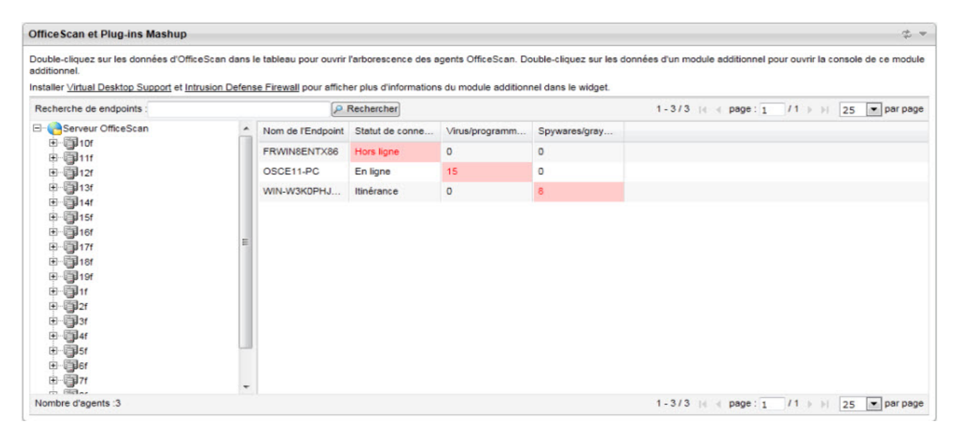


FIGURE 2-13. Widget Mashup d'OfficeScan et des modules additionnels

Ce widget affiche les données pour les programmes de plug-in suivants :

- Intrusion Defense Firewall
- Trend Micro Virtual Desktop Support

Ces programmes de plug-in doivent être activés pour que le widget de mashup affiche les données. Mettez les programmes de plug-in à niveau si des versions plus récentes sont disponibles.

Dans ce widget, vous pouvez effectuer les actions suivantes :

- Choisissez les colonnes s'affichant dans l'arborescence des agents. Cliquez sur l'icône Modifier ( ) dans le coin supérieur droit du widget, puis sélectionnez les colonnes s'affichant sur l'écran.

Tableau 2-6. Colonnes Mashup d'OfficeScan et des modules additionnels

Nom de colonne	Description
Nom de l'ordinateur	Nom de l'Endpoint Cette colonne est toujours disponible et ne peut être supprimée.
Hiérarchie des domaines	Le domaine du endpoint dans l'arborescence des agents OfficeScan
État de la connexion	La connectivité des agents OfficeScan avec leur serveur OfficeScan parent
Virus/programmes malveillants	Le nombre de virus et de programmes malveillants détectés par l'agent OfficeScan
Spyware/Grayware	Le nombre de spywares et graywares détectés par l'agent OfficeScan
Prise en charge de VDI	Indique si le endpoint est une machine virtuelle ou non
Profil sécurité d'IDF	Consultez la documentation IDF pour plus d'informations sur ces colonnes et sur les données qu'elles présentent.
Pare-feu IDF	
État IDF	
DPI IDF	

- Double-cliquez sur les données du tableau. Double-cliquez sur les données OfficeScan pour afficher l'arborescence des agents OfficeScan. Si vous double-

cliquez sur les données d'un programme de plug-in (à l'exception des données de la colonne **Prise en charge de VDI**), l'écran principal de ce programme s'affiche.

- Utilisez l'option de recherche pour trouver chaque endpoint. Vous pouvez saisir un nom d'hôte en totalité ou de façon partielle.

Widget Incidents majeurs de prévention contre la perte de données

Ce widget est disponible uniquement si vous activez la protection des données OfficeScan.

Ce widget affiche le nombre de transmissions d'actifs numériques, quelle que soit l'action (bloquée ou ignorée).

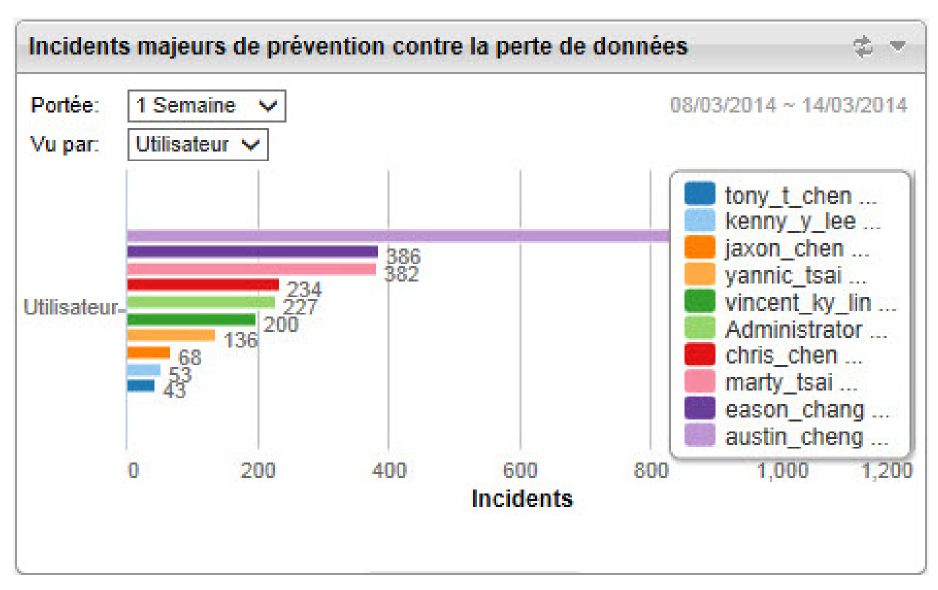


FIGURE 2-14. Widget Incidents majeurs de prévention contre la perte de données

Pour afficher les données :

1. Sélectionnez une période de temps pour les détections. Choisissez parmi :

- **Aujourd'hui**: Détections durant les dernières 24 heures, en incluant l'heure actuelle
- **1 semaine**: Détections durant les 7 derniers jours, en incluant le jour actuel
- **2 semaines**: Détections durant les 14 derniers jours, en incluant le jour actuel
- **1 mois**: Détections durant les 30 derniers jours, en incluant le jour actuel

2. Après avoir sélectionné la période de temps, choisissez parmi :
    - **Utilisateur** : Utilisateurs transmettant le plus souvent des actifs numériques
    - **Canal** : Canaux les plus souvent utilisés afin de transmettre les actifs numériques
    - **Modèle** : Modèles d'actifs numériques ayant déclenché la plupart des détections
    - **Ordinateur** : Ordinateurs ayant transmis le plus souvent des actifs numériques



Remarque

Ce widget affiche un maximum de 10 utilisateurs, canaux, modèles ou ordinateurs.

Widget Incidents de prévention contre la perte de données dans le temps

Ce widget est disponible uniquement si vous activez la protection des données OfficeScan.

Ce widget affiche le nombre de transmissions d'actifs numériques pendant une période donnée. Les transmissions comprennent celles qui sont bloquées ou ignorées (autorisées).

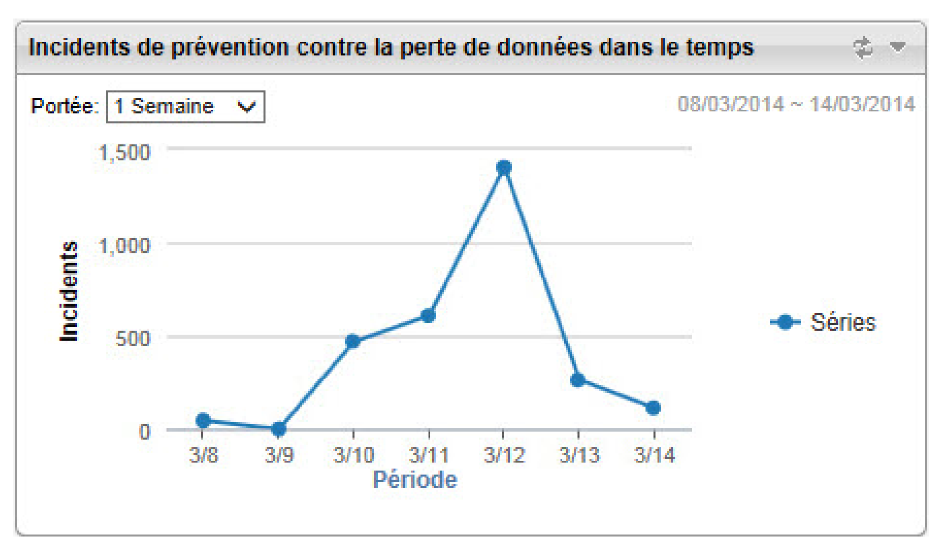


FIGURE 2-15. Widget Incidents de prévention contre la perte de données dans le temps

Pour afficher les données, sélectionnez une période de temps pour les détections. Choisissez parmi :

- **Aujourd'hui** : Détections durant les dernières 24 heures, en incluant l'heure actuelle
- **1 semaine** : Détections durant les 7 derniers jours, en incluant le jour actuel
- **2 semaines** Détections durant les 14 derniers jours, en incluant le jour actuel
- **1 mois** Détections durant les 30 derniers jours, en incluant le jour actuel

Widget Événements de rappel C&C

Le widget **Événements de rappel C&C** affiche toutes les informations relatives aux événements de rappel C&C, y compris la cible de l'attaque et l'adresse source de rappel.

Les administrateurs peuvent choisir de visualiser les informations de rappel C&C à partir d'une liste des serveurs C&C spécifique. Pour choisir la source de la liste (Global Intelligence, Virtual Analyzer), cliquez sur l'icône Modifier ( ) et faites votre sélection dans la liste déroulante **Source de la liste C&C**.

Affichez les données de rappel C&C en sélectionnant les éléments suivants :

- **Hôte compromis** : Affiche les informations C&C les plus récentes par endpoint ciblé

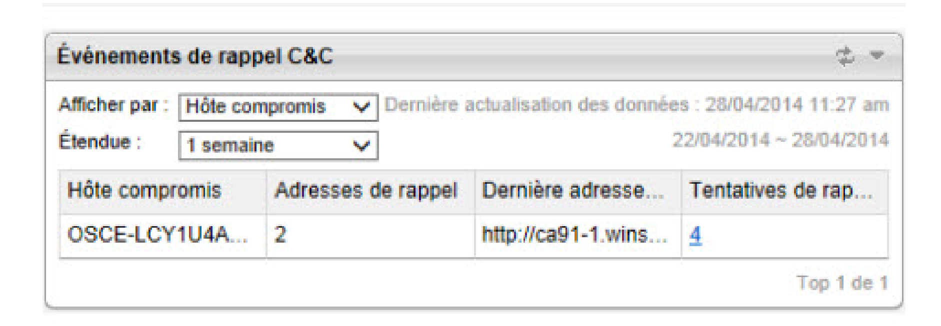


FIGURE 2-16. Widget Événements de rappel C&C affichant des informations sur la cible

TABLEAU 2-7. Informations sur l'hôte compromis

COLONNE	DESCRIPTION
Hôte compromis	Le nom de l'endpoint visé par l'attaque C&C
Adresses de rappel	Le nombre d'adresses de rappel que le endpoint a tenté de contacter
Dernière adresse de rappel	La dernière adresse de rappel que le endpoint a tenté de contacter

Colonne	Description
Tentatives de rappel	Le nombre de fois que le endpoint ciblé a tenté de contacter avec l'adresse de rappel **Remarque** Cliquez sur le lien hypertexte pour ouvrir l'écran **Journaux de rappel C&C** et afficher des informations plus détaillées.

- **Adresse de rappel** : Affiche les informations C&C les plus récentes par adresse de rappel C&C

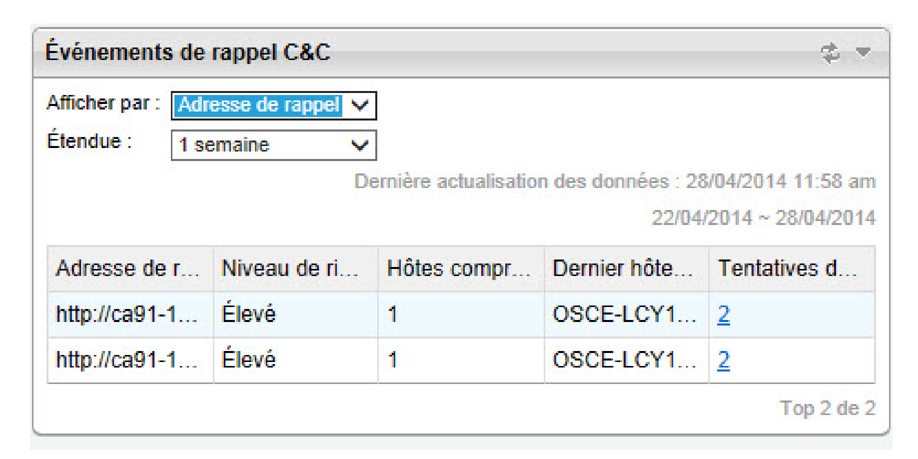


Figure 2-17. Widget Événements de rappel C&C affichant des informations sur les adresses de rappel

Tableau 2-8. Informations d'adresse C&C

Colonne	Description
Adresse de rappel	L'adresse des rappels C&C provenant du réseau

Colonne	Description
Niveau de risque C&C	Le niveau de risque de l'adresse de rappel déterminé soit par la liste Informations globales, soit par la liste Virtual Analyzer
Hôtes compromis	Le nombre de endpoints que l'adresse de rappel a ciblé
Dernier hôte compromis	Le nom du dernier endpoint qui a tenté de contacter l'adresse de rappel C&C
Tentatives de rappel	Le nombre de tentatives de rappels réalisé sur l'adresse du réseau **Remarque** Cliquez sur le lien hypertexte pour ouvrir l'écran **Journaux de rappel C&C** et afficher des informations plus détaillées.

Widget Sources majeures des menaces selon la réputation des sites Web

Ce widget affiche le nombre total de détections de menaces liées à la sécurité effectuées par les services de réputation de sites Web. Les informations sont affichées sur une carte du monde, en fonction de la localisation géographique. Pour obtenir de l'aide sur

l'utilisation de ce widget, cliquez sur le bouton Aide (?) dans la partie supérieure du widget.

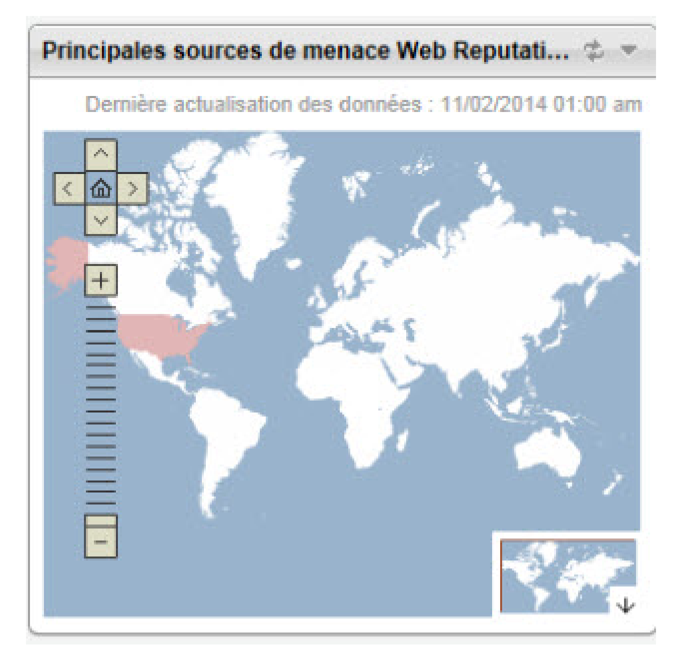


FIGURE 2-18. Widget Sources majeures des menaces selon la réputation des sites Web

Widget Utilisateurs les plus menacés selon la réputation des sites Web

Ce widget affiche le nombre d'utilisateurs infectés par des adresses URL malveillantes détectées par les services de réputation de sites Web. Les informations sont affichées sur une carte du monde, en fonction de la localisation géographique. Pour obtenir de l'aide

sur l'utilisation de ce widget, cliquez sur le bouton Aide (?) dans la partie supérieure du widget.

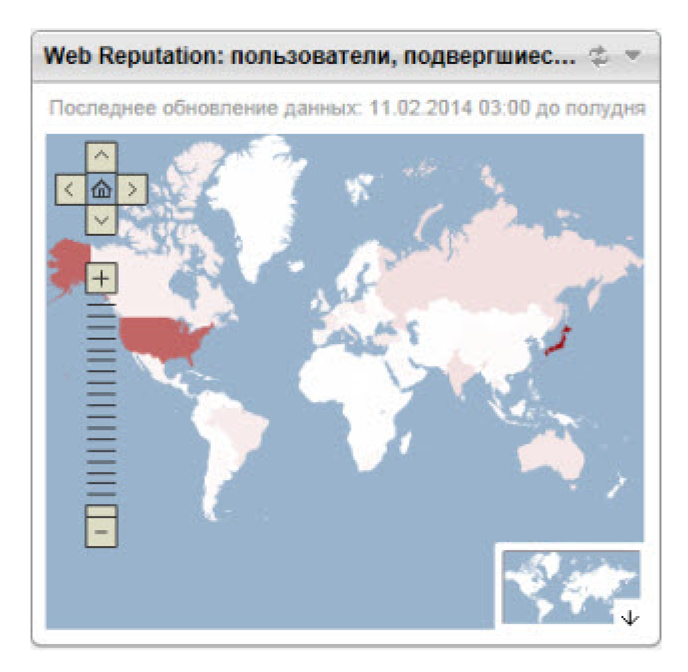


FIGURE 2-19. Widget Utilisateurs les plus menacés selon la réputation des sites Web

Widget Carte des menaces de File Reputation

Ce widget affiche le nombre total de détections de menaces liées à la sécurité effectuées par les services de file reputation. Les informations sont affichées sur une carte du monde, en fonction de la localisation géographique. Pour obtenir de l'aide sur

l'utilisation de ce widget, cliquez sur le bouton Aide (?) dans la partie supérieure du widget.

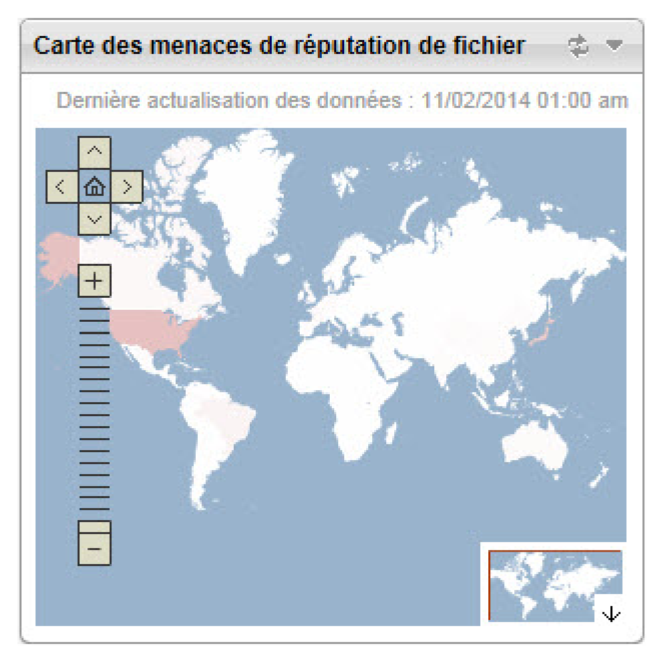


FIGURE 2-20. Widget Carte des menaces de File Reputation

Outil de migration de serveur

OfficeScan fournit l'outil de migration de serveur, qui permet aux administrateurs de copier les paramètres d'anciennes versions d'OfficeScan vers la version actuelle. L'outil de migration de serveur effectue la migration des paramètres suivants :

- Structures de domaine
- Paramètres de scan manuel*
- Paramètres des services complémentaires*
- Liste des spywares/graywares approuvés*

- Paramètres de scan programmé*
- Paramètres de scan en temps réel*
- Paramètres de scan immédiat*
- Paramètres de réputation de sites Web*
- Liste d'URL approuvées*
- Paramètres de surveillance des comportements*
- Paramètres de contrôle des dispositifs*
- Paramètres de prévention contre la perte de données*
- Privilèges et autres paramètres*
- Paramètres généraux de l'agent
- Emplacement de l'Endpoint (ordinateur)
- Stratégies et profils de pare-feu
- Sources Smart Protection
- Programme de mise à jour du serveur
- Source et programmation de mise à jour de l'agent (client)
- Notifications
- Paramètres proxy
- Port de l'agent (client) OfficeScan et Client_LocalServer_Port dans le fichier `ofcscan.ini`



Remarque

- Les paramètres munis d'un astérisque (*) conservent les configurations au niveau du domaine et de la racine.
- L'outil ne sauvegarde pas les listes d'agents OfficeScan du serveur OfficeScan ; seules les structures de domaine sont sauvegardées.
- L'agent OfficeScan effectue uniquement la migration des fonctionnalités disponibles sur l'ancienne version du serveur de l'agent OfficeScan. Pour les fonctionnalités qui n'étaient pas disponibles sur l'ancien serveur, l'agent OfficeScan applique les paramètres par défaut.

Utilisation de l'outil de migration de serveur



Remarque

Cette version d'OfficeScan prend en charge les migrations à partir de la version 10.0 d'OfficeScan ou une version ultérieure.

Les anciennes versions d'OfficeScan peuvent ne pas contenir tous les paramètres disponibles dans la dernière version. OfficeScan applique automatiquement les paramètres par défaut aux fonctionnalités qui n'ont pas été migrées depuis la version précédente du serveur OfficeScan.

Procédure

1. Sur l'ordinateur du serveur OfficeScan 11.0, accédez au répertoire <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\ServerMigrationTool`.

2. Copiez l'outil de migration de serveur sur l'ordinateur du serveur OfficeScan source.



Important

Vous devez utiliser l'outil de migration de serveur OfficeScan 11.0 sur le serveur OfficeScan source afin de vous assurer que toutes les données soient correctement formatées pour le nouveau serveur cible. OfficeScan 11.0 n'est pas compatible avec les versions antérieures de l'outil de migration de serveur.

3. Double-cliquez sur `ServerMigrationTool.exe` pour démarrer l'outil de migration de serveur.

   L'outil de migration de serveur s'ouvre.

4. Pour exporter les paramètres depuis le serveur OfficeScan source :

   a. Spécifiez le dossier de destination à l'aide du bouton **Parcourir**.

   Remarque

   Le nom par défaut du module d'exportation est `OsceMigrate.zip`.

   b. Cliquez sur **Exporter**.

Un message de confirmation s'affiche.

c. Copiez le module d'exportation vers le serveur OfficeScan de destination.

5. Pour importer les paramètres vers le serveur OfficeScan de destination :

   a. Trouvez le module d'exportation à l'aide du bouton **Parcourir**.

   b. Cliquez sur **Importer**.

   Un message d'avertissement s'affiche.

   c. Cliquez sur **Oui** pour continuer.

   Un message de confirmation s'affiche.

6. Vérifiez que le serveur contient tous les paramètres de la version OfficeScan précédente.

7. Déplacez les anciens agents OfficeScan vers le nouveau serveur.

   Pour plus d'informations sur le déplacement d'agents OfficeScan, voir *Déplacement d'agents OfficeScan vers un autre domaine ou serveur OfficeScan à la page 2-62* ou *Agent Mover à la page 14-23*.

Intégration d'Active Directory

Intégrez OfficeScan à votre structure Microsoft™ Active Directory™ pour gérer les agents OfficeScan plus efficacement, affecter des autorisations sur la console Web à l'aide de comptes Active Directory et déterminer les agents sur lesquels aucun logiciel de sécurité n'est installé. Tous les utilisateurs du domaine réseau peuvent bénéficier d'un accès sécurisé à la console OfficeScan. Vous pouvez également affecter un accès limité à certains utilisateurs, même s'ils appartiennent à un autre domaine. Le processus d'authentification et la clé de chiffrement permettent de valider les informations d'authentification des utilisateurs.

Active Directory vous permet de tirer pleinement parti des fonctionnalités suivantes :

- **Administration basée sur les rôles** : affectez des responsabilités administratives spécifiques aux utilisateurs en leur accordant un accès à la console du produit à

l'aide de leurs comptes Active Directory. Pour obtenir des informations détaillées, voir *Administration basée sur les rôles à la page 13-2*.

- **Groupes d'agents personnalisés** : utilisez Active Directory ou des adresses IP pour regrouper manuellement des agents et les mapper sur des domaines de l'arborescence des agents OfficeScan. Pour obtenir des informations détaillées, voir *Regroupement automatique des agents à la page 2-55*.
- **Gestion des serveurs externes** : assurez-vous que les ordinateurs du réseau qui ne sont pas gérés par le serveur OfficeScan respectent les consignes de sécurité de votre société. Pour obtenir des informations détaillées, voir *Conformité de la sécurité pour les endpoints non gérés à la page 14-71*.

Synchronisez manuellement ou périodiquement la structure Active Directory avec le serveur OfficeScan pour garantir la cohérence des données. Pour obtenir des informations détaillées, voir *Synchronisation des données avec les domaines Active Directory à la page 2-39*.

Intégration d'Active Directory dans OfficeScan

Procédure

1. Accédez à **Administration** > **Active Directory** > **Intégration d'Active Directory**.
2. Sous **Domaines Active Directory**, spécifiez le nom du domaine Active Directory.
3. Indiquez les informations d'identification que le serveur OfficeScan Server utilisera lors de la synchronisation des données avec le domaine Active Directory spécifié. Les informations d'identification sont requises si le serveur ne fait pas partie du domaine. Sinon, les informations d'identification sont facultatives. Assurez-vous que ces informations d'identification n'expirent pas ou le serveur ne sera pas en mesure de synchroniser les données.
   a. Cliquez sur **Spécifier les informations d'authentification du domaine**.
   b. Dans la fenêtre contextuelle qui s'affiche, entrez le nom d'utilisateur et le mot de passe. Le nom d'utilisateur peut être spécifié en utilisant l'un des formats suivants :

- `Domaine\Nom d'utilisateur`
- `nomdutilisateur@domaine`

c. Cliquez sur **Enregistrer**.

4. Cliquez sur le bouton (+) pour ajouter des domaines. Spécifiez les informations d'authentification de domaine pour les domaines ajoutés si nécessaire.

5. Cliquez sur le bouton (-) pour supprimer des domaines.

6. Spécifiez les paramètres de chiffrement si vous avez indiqué des informations d'identification de domaine. Par mesure de sécurité, OfficeScan chiffre les informations d'identification que vous avez spécifiées avant de les enregistrer dans la base de données. Lorsqu'OfficeScan synchronise les données avec l'un des domaines spécifiés, il utilise une clé de chiffrement pour déchiffrer les informations d'identification du domaine.

   a. Rendez-vous à la section **Paramètres de chiffrement pour les informations d'identification du domaine**.

   b. Entrez une clé d'encodage qui ne dépasse pas 128 caractères.

   c. Indiquez un fichier dans lequel enregistrer la clé d'encodage. Vous pouvez choisir un format de fichier courant, comme `.txt`. Entrez le nom et le chemin d'accès complets du fichier, comme `C:\AD_Encryption\EncryptionKey.txt`.



AVERTISSEMENT!

Si le fichier est supprimé ou si le chemin d'accès est modifié, OfficeScan ne pourra pas synchroniser les données avec l'ensemble des domaines spécifiés.

7. Choisissez l'une des options suivantes :

   - **Enregistrer** : Enregistrez les paramètres uniquement. La synchronisation des données pouvant accaparer les ressources du réseau, vous pouvez choisir d'enregistrer les paramètres uniquement et de synchroniser plus tard, en heures creuses.
   - **Enregistrer et synchroniser** : enregistre les paramètres et synchronise les données avec les domaines Active Directory.

8. Programmez des synchronisations périodiques. Pour obtenir des informations détaillées, voir *Synchronisation des données avec les domaines Active Directory à la page 2-39*.

Synchronisation des données avec les domaines Active Directory

Synchronisez régulièrement les données aves les domaines Active Directory pour maintenir à jour la structure de l'arborescence des agents OfficeScan et pour interroger les agents non gérés.

Synchronisation manuelle des données avec les domaines Active Directory

Procédure

1. Accédez à **Administration** > **Active Directory** > **Intégration d'Active Directory**.
2. Vérifiez que les informations d'authentification du domaine et les paramètres de chiffrement n'ont pas changé.
3. Cliquez sur **Enregistrer et synchroniser**.

Synchronisation automatique des données avec les domaines Active Directory

Procédure

1. Accédez à **Administration** > **Active Directory** > **Synchronisation programmée**.
2. Sélectionnez **Activer la synchronisation programmée d'Active Directory**.
3. Programmez la synchronisation.



Remarque

Pour des synchronisations quotidiennes, hebdomadaires et mensuelles, la période correspond au nombre d'heures pendant lesquelles OfficeScan synchronise Active Directory avec le serveur OfficeScan.

4. Cliquez sur **Enregistrer**.

L'arborescence des agents OfficeScan

L'arborescence des agents OfficeScan affiche tous les agents (regroupés par domaines) actuellement gérés par le serveur. Les agents sont regroupés par domaines afin de vous permettre de configurer, gérer et appliquer simultanément la même configuration à tous les membres du domaine.

L'arborescence des agents s'affiche dans le cadre principal lorsque vous cliquez sur certaines fonctions du menu principal.

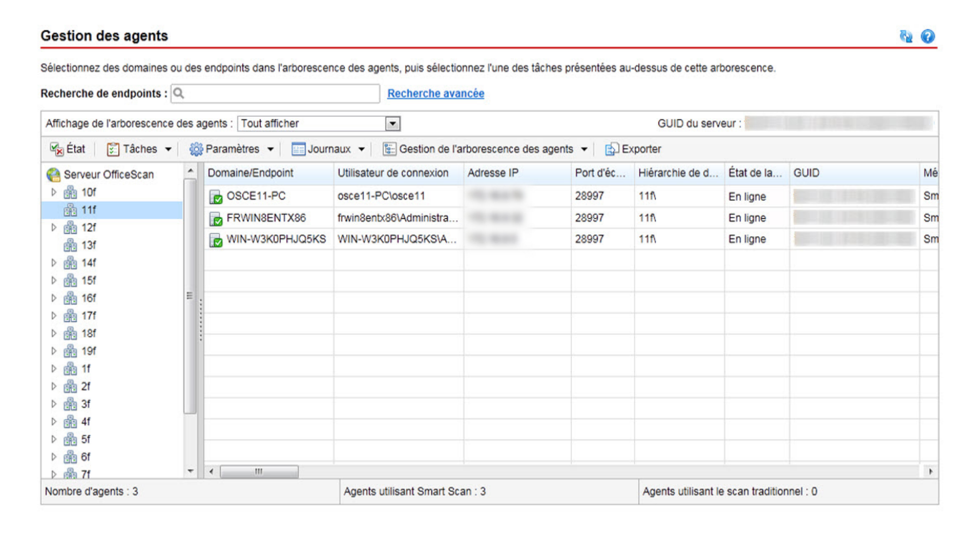


FIGURE 2-21. Arborescence des agents OfficeScan

Icônes de l'arborescence des agents

Les icônes de l'arborescence des agents OfficeScan fournissent des indications visuelles sur le type de endpoint et l'état des agents OfficeScan gérés par OfficeScan.

TABLEAU 2-9. Icônes de l'arborescence des agents OfficeScan

ICÔNE	DESCRIPTION
	Domaine
	Racine
	Agent de mise à jour
	Agent de scan traditionnel
	Smart Scan est disponible sur l'agent OfficeScan
	Smart Scan n'est pas disponible sur l'agent OfficeScan
	Smart Scan est disponible pour l'agent de mise à jour
	Smart Scan n'est pas disponible pour l'agent de mise à jour

Tâches générales de l'arborescence des agents

Les tâches pouvant être effectuées sur l'arborescence des agents sont les suivantes :

Procédure

- Pour sélectionner tous les domaines et agents, cliquez sur l'icône de domaine racine . Lorsque vous sélectionnez l'icône de domaine racine, puis choisissez une tâche

au-dessus de l'arborescence des agents, un écran permettant de configurer les paramètres s'affiche. Sur l'écran, choisissez parmi les options générales suivantes :

- **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.
- **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

- Pour sélectionner plusieurs domaines ou agents adjacents :
    - Dans le panneau de droite, sélectionnez le premier domaine, appuyez sur la touche MAJ et maintenez-la enfoncée, puis cliquez sur le dernier domaine ou agent de la plage.
- Pour sélectionner plusieurs domaines ou agents n'étant pas à la suite les uns des autres, appuyez sur la touche CTRL et maintenez-la enfoncée, puis cliquez sur les domaines ou agents à sélectionner.
- Recherchez un agent à gérer en spécifiant son nom dans le champ **Recherche de endpoints**.

  Une liste de résultats s'affiche dans l'arborescence des agents. Pour disposer de plus d'options de recherche, cliquez sur **Recherche avancée**.



Remarque

Vous ne pouvez pas indiquer d'adresses IPv6 ou IPv4 dans le cadre d'une recherche d'agents spécifiques. Utilisez la recherche avancée pour faire une recherche à partir d'une adresse IPv4 ou IPv6. Pour obtenir des informations détaillées, voir *Options de recherche avancée à la page 2-43*.

- Après avoir sélectionné un domaine, le tableau de l'arborescence des agents se développe pour montrer les agents appartenant au domaine, ainsi que toutes les colonnes contenant des informations correspondant à chaque agent. Pour afficher uniquement un jeu de colonnes connexes, sélectionnez un élément dans l'affichage de l'arborescence des agents.

- **Afficher tout** : affiche toutes les colonnes
- **Mise à jour** : affiche tous les composants et programmes
- **Affichage antivirus** : affiche les composants antivirus
- **Affichage antispyware :** affiche les composants anti-spyware
- **Affichage de la protection des données** : affiche l'état du module de protection des données sur les agents
- **Pare-feu** : affiche les composants de pare-feu
- **Affichage Smart protection** : affiche la méthode de scan utilisée par les agents (scan traditionnel ou Smart Scan) et les composants Smart Protection
- **Agent de mise à jour** : affiche des informations pour tous les agents de mise à jour gérés par le serveur OfficeScan

- Vous pouvez réorganiser les colonnes en faisant glisser leurs titres à d'autres endroits de l'arborescence des agents. OfficeScan sauvegarde automatiquement les nouvelles positions de colonne.
- Vous pouvez trier les agents en fonction des informations contenues dans une colonne en cliquant sur le nom de cette colonne.
- Vous pouvez actualiser l'arborescence des agents en cliquant sur l'icône d'actualisation ( ).
- Vous pouvez afficher des statistiques relatives aux agents sous l'arborescence des agents, par exemple le nombre total d'agents, le nombre d'agents Smart Scan et le nombre d'agents de scan traditionnel.

Options de recherche avancée

Recherchez des agents en fonction des critères suivants :

Procédure

- **Critères de base** : comprend des informations de base sur les endpoints, telles que leur adresse IP, leur système d'exploitation, leur domaine, leur adresse MAC, leur méthode de scan et l'état de leur service de réputation de sites Web
  - La recherche par segment IPv4 requiert une partie d'une adresse IP, commençant par le premier octet. La recherche renvoie tous les endpoints dont l'adresse IP contient l'élément saisi. Par exemple, si vous tapez 10.5, vous trouverez tous les ordinateurs dont l'adresse IP est incluse dans une plage allant de 10.5.0.0 à 10.5.255.255.
  - La recherche par plage d'adresses IPv6 requiert un préfixe et une longueur.
  - La recherche par adresse MAC requiert une plage d'adresses MAC en notation hexadécimale, par exemple 000A1B123C12.
- **Versions du composant** : cochez la case en regard du nom de composant, raffinez le critère en sélectionnant **Antérieur à** ou **Antérieur ou égal à**, puis entrez un numéro de version. Le numéro de version actuel s'affiche par défaut.
- **État** : inclut les paramètres des agents
- Cliquez sur **Rechercher** après avoir spécifié les critères de recherche. Une liste des noms des endpoints répondant aux critères s'affiche dans l'arborescence des agents.

Tâches spécifiques dans l'arborescence des agents

L'arborescence des agents s'affiche lorsque vous accédez à certains écrans de la console Web. Des options de menu propres à l'écran auquel vous accédez s'affichent au-dessus de l'arborescence des agents. Elles vous permettent de réaliser certaines tâches, par exemple la configuration des paramètres des agents ou le lancement de tâches sur les agents. Pour effectuer une tâche quelconque, commencez par sélectionner la cible de la tâche, puis sélectionnez une option de menu.

Les écrans suivants affichent l'arborescence des agents :

- *Écran Gestion des agents à la page 2-45*
- *Écran Prévention des épidémies à la page 2-49*

- *Écran Sélection de l'agent à la page 2-49*
- *Écran Rétrograder à la page 2-50*
- *Écran Journaux des risques de sécurité à la page 2-51*

L'arborescence des agents permet d'accéder aux fonctions suivantes :

- **Recherche de endpoints** : permet de rechercher des endpoints spécifiques en saisissant des critères dans la zone de texte.

Les administrateurs peuvent également rechercher manuellement des endpoints ou des domaines dans l'arborescence des agents. Les informations propres à chaque ordinateur s'affichent sur la droite du tableau.

Écran Gestion des agents

Pour afficher cet écran, accédez à **Agents** > **Gestion des agents**.

Vous pouvez gérer les paramètres généraux des agents et afficher des informations relatives à l'état d'agents spécifiques (par exemple **Utilisateur de connexion**, **Adresse IP** et **État de la connexion**) sur l'écran **Gestion des agents**.

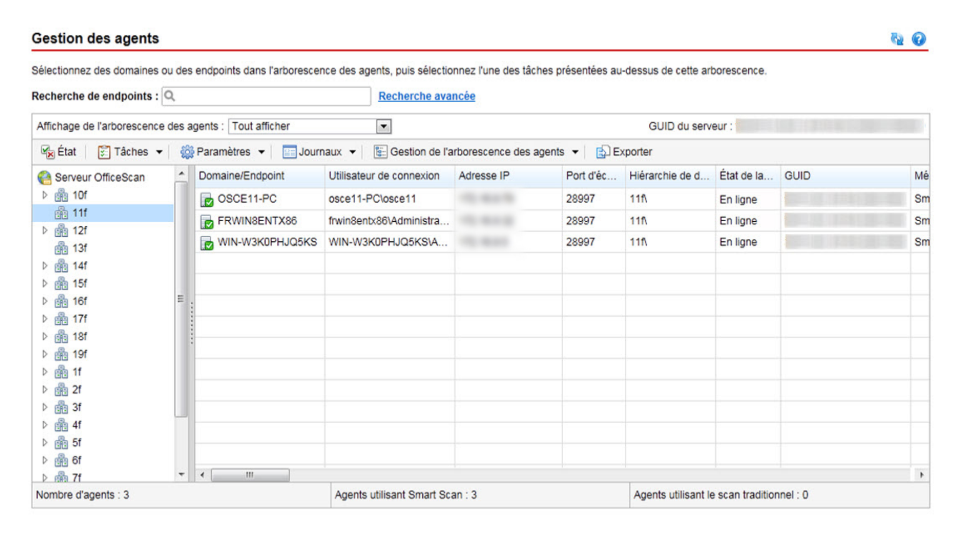


FIGURE 2-22. Écran Gestion des agents

Le tableau suivant répertorie les tâches que vous pouvez effectuer :

TABLEAU 2-10. Tâches de Gestion des agents

BOUTON DE MENU	TÂCHE
État	Afficher des informations détaillées sur les agents. Pour obtenir des informations détaillées, voir *Affichage des informations sur les agents OfficeScan à la page 14-56*.
Tâches	• Exécuter un scan immédiat sur les ordinateurs des agents. Pour obtenir des informations détaillées, voir *Exécution du scan immédiat à la page 7-26*. • Désinstaller l'agent. Pour obtenir des informations détaillées, voir *Désinstallation de l'agent OfficeScan depuis la console Web à la page 5-74*. • Restaurer des fichiers suspects détectés. Pour obtenir des informations détaillées, voir *Restauration de fichiers mis en quarantaine à la page 7-46*. • Restaurer des spywares/graywares. Pour obtenir des informations détaillées, voir *Restauration des spywares/ graywares à la page 7-55*.

Bouton de menu	Tâche
Paramètres	• Configurer les paramètres de scan. Pour obtenir des informations détaillées, reportez-vous aux sections suivantes : • *Types de méthodes de scan à la page 7-9* • *Scan manuel à la page 7-19* • *Scan en temps réel à la page 7-16* • *Scan programmé à la page 7-21* • *Scan immédiat à la page 7-24* • Configurer les paramètres de réputation de sites Web. Pour obtenir des informations détaillées, voir *Stratégies de réputation de sites Web à la page 11-5*. • Configurer les paramètres de connexion suspecte. Pour obtenir des informations détaillées, consultez la section *Configuration des paramètres de connexion suspecte à la page 11-15*. • Configurer les paramètres de surveillance des comportements. Pour obtenir des informations détaillées, voir *Surveillance des comportements à la page 8-2*. • Configurer les paramètres de contrôle des dispositifs. Pour obtenir des informations détaillées, voir *Contrôle des dispositifs à la page 9-2*. • Configurer les stratégies de prévention contre la perte de données. Pour obtenir des informations détaillées, voir *Configuration de la stratégie de prévention contre la perte de données à la page 10-46*. • Attribuer à des agents le rôle d'agent de mise à jour. Pour obtenir des informations détaillées, voir *Configuration de l'agent de mise à jour à la page 6-60*. • Configurer les privilèges et d'autres paramètres des agents. Pour obtenir des informations détaillées, voir *Configuration des privilèges des agents et d'autres paramètres à la page 14-93*. • Activer ou désactiver les services des agents OfficeScan. Pour obtenir des informations détaillées, voir *Services de l'agent OfficeScan à la page 14-7*. • Modifier la liste de spywares/graywares approuvés. Pour obtenir des informations détaillées, voir *Liste des spywares/graywares approuvés à la page 7-52*. • Importer et exporter les paramètres des agents. Pour obtenir des informations détaillées, voir *Importation et exportation des paramètres d'un agent à la page 14-56*.

BOUTON DE MENU	TÂCHE
Journaux	Afficher les journaux suivants : • Journaux de virus/programmes malveillants (pour plus d'informations, voir *Affichage des journaux de virus/programmes malveillants à la page 7-92*) • Journaux de spywares/graywares (pour plus d'informations, voir *Affichage des journaux de spywares/graywares à la page 7-101*) • Journaux de pare-feu (pour plus d'informations, voir *Journaux de pare-feu à la page 12-30*) • Journaux de réputation de sites Web (pour plus d'informations, voir *Journaux des menaces Web à la page 11-24*) • Journaux de connexion suspecte (pour plus d'informations, voir *Affichage des journaux des connexions suspectes à la page 11-27*) • Journaux de rappel C&C (pour plus de détails, veuillez consulter *Affichage des journaux de rappel C&C à la page 11-26*.) • Journaux de surveillance des comportements (pour plus d'informations, voir *Journaux de surveillance des comportements à la page 8-15*) • Journaux DLP (pour plus d'informations, voir *Journaux de prévention contre la perte de données à la page 10-56*) • Journaux de contrôle des dispositifs (pour plus d'informations, voir *Journaux de contrôle des dispositifs à la page 9-19*) Suppression des journaux. Pour obtenir des informations détaillées, voir *Gestion du journal à la page 13-36*.
Gestion de l'arborescence des agents	Gérer l'arborescence des agents. Pour obtenir des informations détaillées, voir *Tâches de regroupement des agents à la page 2-60*.
Exporter	Exporter une liste des agents dans un fichier au format `.csv` (valeurs séparées par des virgules).

Écran Prévention des épidémies

Pour afficher cet écran, accédez à **Agents** > **Prévention des épidémies**.

Indiquez et activez les paramètres de prévention des épidémies dans l'écran **Prévention des épidémies**. Pour obtenir des informations détaillées, voir *Configuration de la prévention des épidémies de risques liés à la sécurité à la page 7-111*.

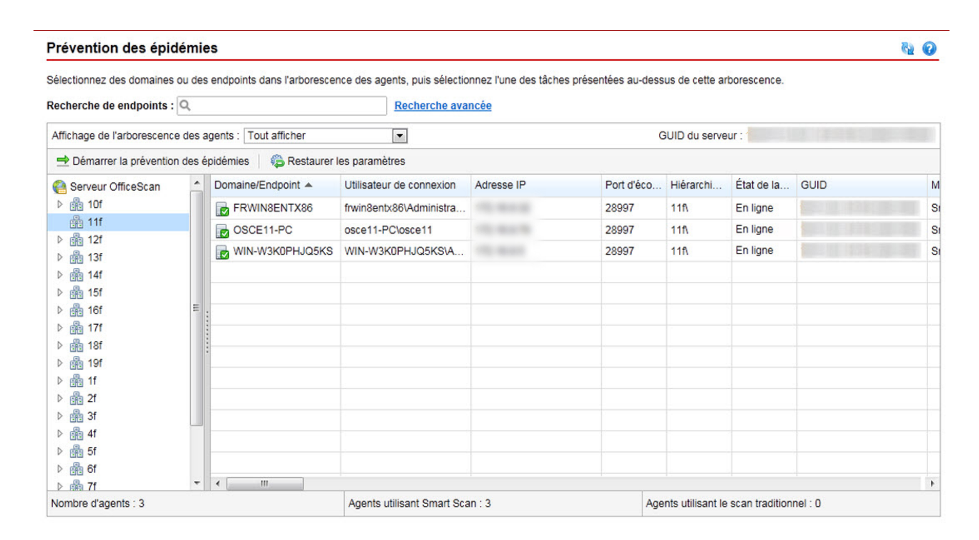


FIGURE 2-23. Écran Prévention des épidémies

Écran Sélection de l'agent

Pour afficher cet écran, accédez à **Mises à jour** > **Agents** > **Mise à jour manuelle**. Cliquez sur **Sélectionner manuellement les agents**, puis cliquez sur **Sélectionner**.

Lancez la mise à jour manuelle à partir de l'écran **Sélection de l'agent**. Pour obtenir des informations détaillées, voir *Mises à jour manuelles des agents OfficeScan à la page 6-49*.

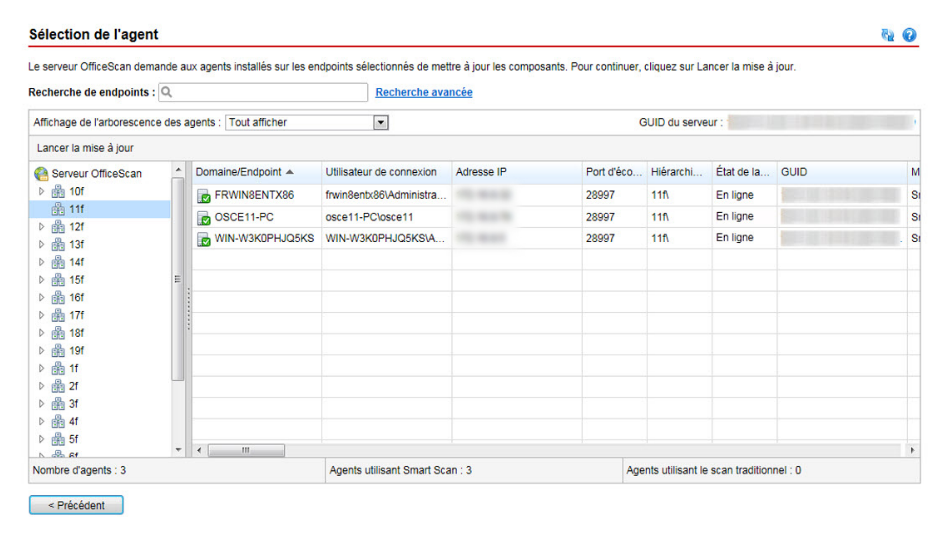


FIGURE 2-24. Écran Sélection de l'agent

Écran Rétrograder

Pour afficher cet écran, accédez à **Mises à jour** > **Rétrograder**. Cliquez sur **Synchroniser avec le serveur**.

Rétrogradez les composants des agents dans l'écran **Rétrograder**. Pour obtenir des informations détaillées, voir *Rétrogradation des composants des agents OfficeScan à la page 6-57*.

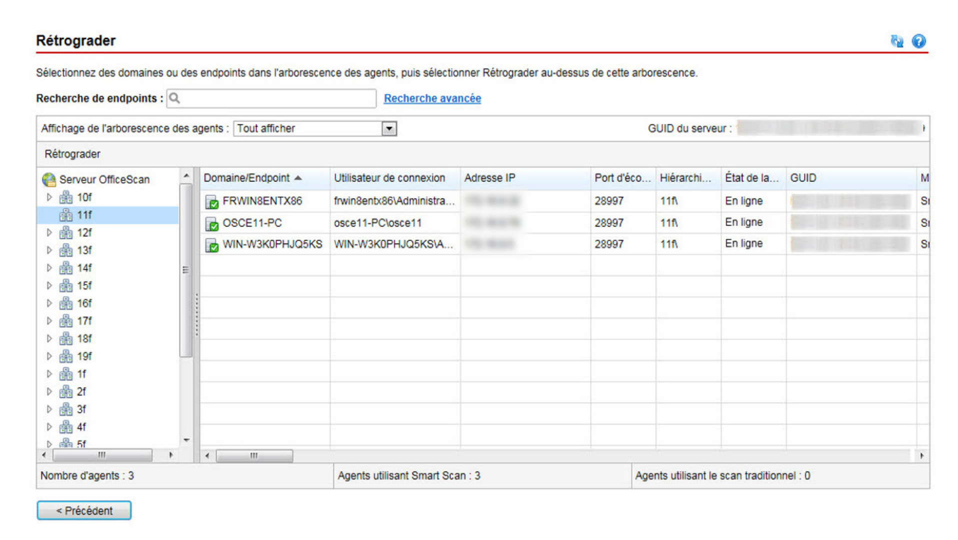


FIGURE 2-25. Écran Rétrograder

Écran Journaux des risques de sécurité

Pour afficher cet écran, accédez à **Journaux** > **Agents** > **Risques de sécurité**.

Affichez et gérez les journaux dans l'écran **Journaux des risques de sécurité**.

Figure 2-26. Écran Journaux des risques de sécurité

Effectuez les actions suivantes :

1. Affichage des journaux envoyés au serveur par les agents. Pour plus d'informations, voir :

- *Affichage des journaux de virus/programmes malveillants à la page 7-92*
- *Affichage des journaux de spywares/graywares à la page 7-101*
- *Affichage des journaux du pare-feu à la page 12-30*
- *Affichage de journaux de réputation de sites Web à la page 11-25*
- *Affichage des journaux des connexions suspectes à la page 11-27*
- *Affichage des journaux de rappel C&C à la page 11-26*
- *Affichage des journaux de surveillance des comportements à la page 8-16*
- *Affichage des journaux de contrôle des dispositifs à la page 9-19*

- *Affichage des journaux de prévention contre la perte de données à la page 10-57*

2. Suppression des journaux. Pour obtenir des informations détaillées, voir *Gestion du journal à la page 13-36*.

Domaines OfficeScan

Un domaine OfficeScan est un groupe d'agents partageant une configuration commune et exécutant des tâches similaires. En regroupant les agents par domaines, vous pouvez configurer, gérer et appliquer la même configuration à tous les membres du domaine. Pour plus d'informations sur le regroupement des agents, voir *Regroupement des agents à la page 2-53*.

Regroupement des agents

Utilisez le regroupement des agents pour créer (manuellement ou automatiquement) et gérer des domaines dans l'arborescence des agents OfficeScan.

Il est possible de regrouper les agents dans des domaines selon deux méthodes.

Tableau 2-11. Méthodes de regroupement des agents

Méthode	Regroupement des agents	Descriptions
Manuelle	• Domaine NetBIOS • Domaine Active Directory • Domaine DNS	Le regroupement manuel des agents définit le domaine auquel un agent nouvellement installé doit appartenir. Lorsque l'agent apparaît dans l'arborescence des agents, vous pouvez le déplacer vers un autre domaine ou serveur OfficeScan. Le regroupement manuel des agents permet également de créer, de gérer et de supprimer des domaines de l'arborescence des agents. Pour obtenir des informations détaillées, voir *Regroupement manuel des agents à la page 2-54*.

MÉTHODE	REGROUPEMENT DES AGENTS	DESCRIPTIONS
Automatique	Groupes d'agents personnalisés	Le regroupement automatique des agents s'appuie sur des règles pour trier les agents dans l'arborescence des agents. Après avoir défini ces règles, vous pouvez accéder à l'arborescence des agents afin de trier manuellement les agents ou autoriser OfficeScan à les trier automatiquement lorsqu'un événement particulier a lieu ou à des intervalles programmées. Pour obtenir des informations détaillées, voir *Regroupement automatique des agents à la page 2-55*.

Regroupement manuel des agents

OfficeScan n'utilise ce paramètre que lors de nouvelles installations d'agents. Le programme d'installation vérifie le domaine réseau auquel appartient le endpoint cible. Si le nom de domaine existe déjà dans l'arborescence des agents, OfficeScan regroupe l'agent du endpoint cible sous ce domaine et applique les paramètres configurés pour ce dernier. Si le nom de domaine n'existe pas, OfficeScan ajoute le domaine à l'arborescence des agents, regroupe l'agent sous ce domaine, puis applique les paramètres racine au domaine et à l'agent.

Configuration du regroupement manuel des agents

Procédure

1. Accédez à **Agents** > **Regroupement des agents**.
2. Spécifiez la méthode de regroupement des agents :
   - Domaine NetBIOS
   - Domaine Active Directory
   - Domaine DNS
3. Cliquez sur **Enregistrer**.

Que faire ensuite

Pour gérer des domaines et les agents regroupés sous ces domaines, exécutez les tâches ci-dessous :

- Ajouter un domaine
- Supprimer un domaine ou un agent
- Renommer un domaine
- Déplacer un seul agent vers un autre domaine

Pour obtenir des informations détaillées, voir *Tâches de regroupement des agents à la page 2-60*.

Regroupement automatique des agents

Le regroupement automatique des agents s'appuie sur des règles définies selon des adresses IP ou des domaines Active Directory. Si une règle définit une adresse IP ou une plage d'adresses IP, le serveur OfficeScan regroupera les agents dont l'adresse IP correspond à un domaine spécifique dans l'arborescence des agents. De même, si une règle définit un ou plusieurs domaines Active Directory, le serveur OfficeScan regroupera les agents appartenant à un domaine Active Directory particulier dans un domaine spécifique dans l'arborescence des agents.

Les agents n'appliquent qu'une règle à la fois. Attribuez des priorités aux règles de manière que, si plusieurs règles sont valables pour un agent, celle dont la priorité est la plus élevée s'applique.

Configuration du regroupement automatique des agents

Procédure

1. Accédez à **Agents** > **Regroupement des agents**.
2. Dans la section **Regroupement des agents**, sélectionnez **Groupes d'agents personnalisés**.
3. Accédez à la section **Regroupement automatique des agents**.

4. Pour commencer à créer des règles, cliquez sur **Ajouter**, puis sélectionnez **Active Directory** ou **Adresse IP**.

    - Si vous avez sélectionné **Active Directory**, consultez les instructions de configuration dans *Définition d'une règle de regroupement des agents par domaines Active Directory à la page 2-57*.

    - Si vous avez sélectionné **Adresse IP**, consultez les instructions de configuration dans *Définition de règles de regroupement des agents par adresses IP à la page 2-58*.

5. Si vous avez créé plus d'une règle, attribuez une priorité aux règles en exécutant ces étapes :

    a. Sélectionnez une règle.

    b. Sous la colonne **Priorité de regroupement**, cliquez sur l'une des flèches pour déplacer la règle vers le haut ou le bas de la liste. Le numéro ID de la règle change pour indiquer cette nouvelle position.

6. Pour utiliser les règles lors du tri des agents :

    a. Cochez les cases pour les règles que vous souhaitez utiliser.

    b. Activez les règles en définissant la commande **État** sur **Activé**.



Remarque

Si vous ne cochez pas la case correspondant à une règle ou si vous désactivez une règle, cette dernière ne sera pas utilisée lors du tri des agents dans l'arborescence des agents. Par exemple, si la règle indique qu'un agent doit être déplacé vers un nouveau domaine, cet agent reste dans son domaine actuel.

7. Spécifiez un calendrier de tri dans la section **Création de domaine programmée**.

    a. Sélectionnez **Activer la création de domaine programmée**.

    b. Spécifiez le programme sous **Création de domaine programmée**.

8. Sélectionnez l'une des options suivantes :

    - **Enregistrer et créer le domaine maintenant** : Choisissez cette option si vous avez spécifié de nouveaux domaines dans *Définition de règles de regroupement*

des agents par adresses IP à la page 2-58, étape 7 ou dans *Définition d'une règle de regroupement des agents par domaines Active Directory à la page 2-57*, étape 7.

- **Enregistrer** : Choisissez cette option si vous n'avez pas spécifié de nouveaux domaines ou si vous souhaitez créer de nouveaux domaines uniquement lors de l'exécution du tri des agents.



Remarque

Le tri des agents ne débute pas après l'exécution de cette étape.

Définition d'une règle de regroupement des agents par domaines Active Directory

Assurez-vous que vous avez configuré les paramètres d'intégration d'Active Directory avant d'exécuter les étapes de la procédure ci-dessous. Pour obtenir des informations détaillées, voir *Intégration d'Active Directory à la page 2-36*.

Procédure

1. Accédez à **Agents** > **Regroupement des agents**.
2. Dans la section **Regroupement des agents**, sélectionnez **Groupes d'agents personnalisés**.
3. Accédez à la section **Regroupement automatique des agents**.
4. Cliquez sur **Ajouter**, puis sélectionnez **Active Directory**.

   Un nouvel écran s'affiche.
5. Sélectionnez **Autoriser le groupage**.
6. Indiquez un nom pour la règle.
7. Sous **Source d'Active Directory**, sélectionnez le(s) domaine(s) ou sous-domaine(s) Active Directory.

8. Sous **Arborescence des agents**, sélectionnez un domaine OfficeScan existant sur lequel sont mappés les domaines Active Directory. Si le domaine OfficeScan souhaité n'existe pas, effectuez les étapes suivantes :

    a. Passez la souris sur un domaine OfficeScan particulier et cliquez sur l'icône d'ajout de domaine (+).

    b. Saisissez le nom de domaine dans la zone de texte prévue à cet effet.

    c. Cliquez sur la coche en regard de la zone de texte. Le nouveau domaine est ajouté et est automatiquement sélectionné.

9. (Facultatif) Sélectionnez **Dupliquer la structure Active Directory dans l'arborescence des agents OfficeScan**. Cette option duplique la hiérarchie des domaines Active Directory sélectionnés dans le domaine OfficeScan sélectionné.

10. Cliquez sur **Enregistrer**.

Définition de règles de regroupement des agents par adresses IP

Créez des groupes d'agents personnalisés à l'aide d'adresses IP réseau pour trier les agents de l'arborescence des agents OfficeScan. Cette fonctionnalité peut aider les administrateurs à organiser l'arborescence des agents OfficeScan avant l'enregistrement d'un agent auprès du serveur OfficeScan.

Procédure

1. Accédez à **Agents** > **Regroupement des agents**.

2. Dans la section **Regroupement des agents**, sélectionnez **Groupes d'agents personnalisés**.

3. Accédez à la section **Regroupement automatique des agents**.

4. Cliquez sur **Ajouter**, puis sélectionnez **Adresse IP**.

    Un nouvel écran s'affiche.

5. Sélectionnez **Autoriser le groupage**.

6. Spécifiez un nom pour le regroupement.
7. Spécifiez l'un des éléments suivants :
   - Une adresse IPv4 ou IPv6 unique
   - Une plage d'adresse IPv4
   - Un préfixe et une longueur IPv6



Remarque

Si les adresses IPv4 et IPv6 d'un agent à double pile appartiennent à deux groupes d'agents distincts, l'agent sera regroupé sous le groupe IPv6. Si le protocole IPv6 est désactivé sur l'ordinateur hôte de l'agent, ce dernier ira dans le groupe IPv4.

8. Sélectionnez le domaine OfficeScan sur lequel l'adresse IP ou la plage d'adresses IP est mappée. Si le domaine n'existe pas, effectuez ce qui suit :
   a. Passez la souris n'importe où sur l'arborescence des agents et cliquez sur l'icône d'ajout de domaine.

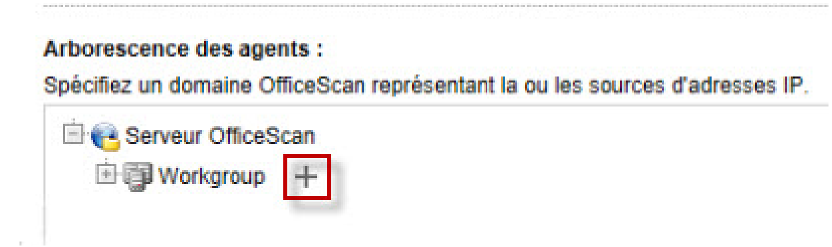


FIGURE 2-27. Icône d'ajout de domaine

   b. Saisissez le domaine dans la zone de texte prévue à cet effet.
   c. Cliquez sur la coche en regard de la zone de texte. Le nouveau domaine est ajouté et est automatiquement sélectionné.
9. Cliquez sur **Enregistrer**.

Tâches de regroupement des agents

Vous pouvez effectuer les tâches suivantes lors du regroupement des agents dans des domaines :

- Ajouter un domaine. Voir *Ajout d'un domaine à la page 2-60* pour plus d'informations.
- Supprimer un domaine ou un agent. Voir *Suppression d'un domaine ou d'un agent à la page 2-61* pour plus d'informations.
- Renommer un domaine. Voir *Attribution d'un nouveau nom à un domaine à la page 2-62* pour plus d'informations.
- Déplacer un seul agent vers un autre domaine ou serveur OfficeScan. Voir *Déplacement d'agents OfficeScan vers un autre domaine ou serveur OfficeScan à la page 2-62* pour plus d'informations.
- Supprimer un domaine ou un agent. Voir *Suppression d'un domaine ou d'un agent à la page 2-61* pour plus d'informations.

Ajout d'un domaine

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Cliquez sur **Gestion de l'arborescence des agents** > **Ajouter un domaine**.
3. Saisissez un nom pour le domaine que vous souhaitez ajouter.
4. Cliquez sur **Ajouter**.

   Le nouveau domaine apparaît dans l'arborescence des agents.
5. (Facultatif) Créez des sous-domaines.

   a. Sélectionnez le domaine parent.

   b. Cliquez sur **Gestion de l'arborescence des agents** > **Ajouter un domaine**.

c. Saisissez le nom de sous-domaine.

Suppression d'un domaine ou d'un agent

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, sélectionnez :
   - Un ou plusieurs domaines
   - Un, plusieurs ou tous les agents appartenant à un domaine
3. Cliquez sur **Gestion de l'arborescence des agents** > **Supprimer un domaine/agent**.
4. Pour supprimer un domaine vide, cliquez sur **Supprimer un domaine/agent**. Si le domaine contient des agents et que vous cliquez sur **Supprimer un domaine/agent**, le serveur OfficeScan crée de nouveau le domaine et regroupe tous les agents sous ce domaine la prochaine fois que ces agents se connectent au serveur OfficeScan. Avant de supprimer le domaine, procédez comme suit :

   a. Déplacez les agents vers d'autres domaines. Pour déplacer des agents vers d'autres domaines, faites-les glisser dans les domaines souhaités.

   b. Supprimez tous les agents.
5. Pour supprimer un seul agent, cliquez sur **Supprimer un domaine/agent**.


Remarque

La suppression d'un agent OfficeScan de l'arborescence des agents ne le supprime pas du endpoint sur lequel il se trouve. L'agent OfficeScan peut toujours effectuer des tâches indépendantes du serveur, telles que la mise à jour des composants. Le serveur n'est cependant pas informé de l'existence de l'agent et ne peut donc pas lui envoyer de notifications, ni y déployer de configurations.

Attribution d'un nouveau nom à un domaine

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Sélectionnez un domaine dans l'arborescence des agents.
3. Cliquez sur **Gestion de l'arborescence des agents** > **Renommer un domaine**.
4. Entrez un nouveau nom pour le domaine.
5. Cliquez sur **Renommer**.

   Le nouveau nom du domaine apparaît dans l'arborescence des agents.

Déplacement d'agents OfficeScan vers un autre domaine ou serveur OfficeScan

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, sélectionnez un, plusieurs ou tous les agents.
3. Cliquez sur **Gestion de l'arborescence des agents** > **Déplacer un agent**.
4. Pour déplacer des agents vers un autre domaine :
   - Sélectionnez **Déplacer le ou les agents sélectionnés vers un autre domaine**.
   - Sélectionnez le domaine.
   - (Facultatif) Appliquez aux agents les paramètres du nouveau domaine.



Conseil

Vous pouvez également faire glisser les agents vers un autre domaine dans l'arborescence des agents.

5. Pour déplacer des agents vers un autre serveur OfficeScan :

    - Sélectionnez **Déplacer le ou les agents sélectionnés vers un autre serveur OfficeScan**.
    - Saisissez le nom ou l'adresse IPv4/IPv6 et le numéro de port HTTP du serveur.

6. Cliquez sur **Déplacer**.



Chapitre 3

Démarrage de la protection des données

Ce chapitre explique comment installer et activer le module Protection des données.

Les rubriques sont les suivantes :

Installation de la protection des données

Le module de protection des données intègre les fonctions suivantes :

- **Prévention contre la perte de données (DLP)** : empêche toute transmission non autorisée d'actifs numériques
- **Contrôle des dispositifs** : Régulation de l'accès aux périphériques externes



Remarque

OfficeScan dispose d'une fonction prête à l'emploi de contrôle des dispositifs, qui régule l'accès aux dispositifs fréquemment utilisés comme les périphériques de stockage USB. Le contrôle des dispositifs, qui fait partie intégrante du module de protection des données, élargit la portée des dispositifs contrôlés. Pour obtenir la liste des dispositifs surveillés, voir *Contrôle des dispositifs à la page 9-2*.

La prévention contre la perte de données et le contrôle des dispositifs sont des fonctionnalités natives OfficeScan mais fournies sous des licences distinctes. Une fois le serveur OfficeScan installé, ces fonctionnalités sont disponibles, mais elles ne sont pas exécutables et ne peuvent pas être déployées sur des agents. L'installation de la protection des données implique le téléchargement d'un fichier depuis le serveur ActiveUpdate (ou depuis une source de mise à jour personnalisée, si définie). Une fois le fichier intégré au serveur OfficeScan, vous pouvez activer la licence de protection de données pour que ses fonctions soient totalement opérationnelles. L'installation et l'activation sont exécutées à partir de **Plug-in Manager**.



Important

- Vous n'avez pas besoin d'installer le module Protection des données si le logiciel Trend Micro Data Loss Prevention est déjà installé et qu'il s'exécute aux endpoints.
- Le module de protection des données peut être installé sur un gestionnaire IPv6 Plug-in Manager pur. Toutefois, seule la fonctionnalité de contrôle des dispositifs peut être déployée sur les agents IPv6 purs. La fonctionnalité de prévention contre la perte de données ne s'exécute pas sur les agents IPv6 purs.

Installation de la protection des données

Procédure

1. Ouvrez la console Web OfficeScan, puis cliquez sur **Modules additionnels** dans le menu principal.

2. Dans l'écran **Plug-in Manager**, accédez à la section **Protection des données OfficeScan** et cliquez sur **Télécharger**.

   La taille du fichier à télécharger s'affiche en regard du bouton **Télécharger**.

   Plug-In Manager stocke le fichier téléchargé dans le répertoire <*dossier d'installation du serveur*>`\PCCSRV\Download\Product`.

   Remarque

   Si Plug-in Manager ne peut pas télécharger le fichier, il relance automatiquement le téléchargement après 24 heures. Pour lancer manuellement le téléchargement du fichier par Plug-in Manager, redémarrez le service Plug-in Manager de OfficeScan depuis Microsoft Management Console.

3. Surveillez la progression du téléchargement.

   Vous pouvez naviguer dans une autre fenêtre pendant le téléchargement.

   Si vous rencontrez des problèmes lors du téléchargement du fichier, consultez les journaux de mise à jour du serveur sur la console Web OfficeScan. Dans le menu principal, cliquez sur **Journaux** > **Mise à jour du serveur**.

   Une fois le fichier téléchargé par Plug-in Manager, la protection des données OfficeScan s'affiche dans un nouvel écran.

   Remarque

   Si la protection des données OfficeScan ne s'affiche pas, consultez les causes et les solutions dans la section *Dépannage de Plug-in Manager à la page 15-12*.

4. Pour installer Protection des données OfficeScan immédiatement, cliquez sur **Installer**, ou pour l'installer ultérieurement, exécutez ce qui suit :

   a. Cliquez sur **Installer ultérieurement**.

b. Ouvrez la fenêtre **Plug-in Manager**.

c. Accédez à la section **Protection des données OfficeScan**, puis cliquez sur **Installer**.

5. Lisez attentivement le contrat de licence, puis acceptez ses termes en cliquant sur **Accepter**.

   L'installation démarre.

6. Surveillez la progression de l'installation. Après l'installation, la version de la protection des données OfficeScan s'affiche.

Licence de protection des données

Affichez, activez et renouvelez la licence de protection des données depuis Plug-in Manager.

Obtenez un code d'activation auprès de Trend Micro, puis utilisez-le afin d'activer la licence.

Activation de la licence d'un module additionnel

Procédure

1. Ouvrez la console Web OfficeScan, puis cliquez sur **Modules additionnels** dans le menu principal.

2. Sur l'écran **Plug-in Manager**, accédez à la section des modules additionnels et cliquez sur **Gestion de programme**.

   L'écran **Nouveau code d'activation de la licence du produit** s'affiche.

3. Saisissez ou copiez-collez le code d'activation dans les champs de texte.

4. Cliquez sur **Enregistrer**.

La console du module additionnel s'affiche.

Affichage et renouvellement des informations sur la licence

Procédure

1. Ouvrez la console Web OfficeScan, puis cliquez sur **Modules additionnels** dans le menu principal.

2. Sur l'écran **Plug-in Manager**, accédez à la section des modules additionnels et cliquez sur **Gestion de programme**.

3. Dans la console du module additionnel, accédez au lien hypertexte **Afficher les informations de licence**.

   Le lien hypertexte **Afficher les informations de licence** ne se trouve pas au même endroit pour tous les modules additionnels. Reportez-vous à la documentation de chaque module additionnel pour plus de détails.

4. Consultez les informations suivantes relatives à la licence dans l'écran qui s'ouvre.

Option	Description
État	Affiche « Activé », « Non activé » ou « Expiré ».
Version	Indique si la version est « Complète » ou d'« Évaluation ». **Remarque** Si la version finale et la version d'évaluation sont activées à la fois, seul « Complète » s'affiche.
Sièges	Affiche le nombre de endpoints pouvant être gérés par le module additionnel.
Date d'expiration du contrat de licence	Si un module additionnel dispose de plusieurs licences, la dernière date d'expiration s'affiche.

Option	Description
	Par exemple, si les dates d'expiration de la licence sont le 31/12/11 et le 30/06/11, la date qui s'affiche est le 31/12/11.
code d'activation	Affiche le code d'activation
Messages de rappel	Selon la version actuelle de votre licence, le module additionnel affiche des messages de rappel relatifs à la date d'expiration de la licence, soit durant la période de grâce (version complète uniquement), soit lorsque la licence expire.



Remarque

La durée de la période de grâce varie selon les régions. Consultez un représentant de Trend Micro pour connaître la période de grâce d'un module additionnel.

Lorsque la licence d'un module additionnel expire, ce dernier continue de fonctionner, mais plus aucune mise à jour n'a lieu et l'assistance n'est plus disponible.

5. Cliquez sur **Afficher le détail de la licence en ligne** pour afficher les informations relatives à la licence actuelle sur le site Web de Trend Micro.

6. Pour rafraîchir l'écran avec les dernières informations de licence, cliquez sur **Informations sur la mise à jour**.

7. Cliquez sur **Nouveau code d'activation** pour ouvrir l'écran **Nouveau code d'activation de la licence du produit**.

   Pour obtenir des informations détaillées, consultez la section *Activation de la licence d'un module additionnel à la page 3-4*.

Déploiement de la protection des données sur les agents OfficeScan

Déployez le module Protection des données sur les agents OfficeScan après activation de sa licence. Après le déploiement, les agents OfficeScan pourront utiliser la prévention contre la perte de données et le contrôle des dispositifs.



Important

- Par défaut, le module est désactivé sur Windows Server 2003, Windows Server 2008 et Windows Server 2012 afin d'éviter tout impact sur les performances de la machine hôte. Si vous souhaitez activer le module, surveillez constamment les performances du système et effectuez les actions nécessaires lorsque vous remarquez une baisse de performances.



Remarque

Vous pouvez activer et désactiver le module à partir de la console Web. Pour obtenir des informations détaillées, consultez la section *Services de l'agent OfficeScan à la page 14-7*.

- Si le logiciel Trend Micro Data Loss Prevention existe déjà au endpoint, OfficeScan ne le remplacera pas par le module de protection des données.
- Seul le contrôle des dispositifs peut être déployé sur des agents IPv6 purs. La prévention contre la perte de données ne fonctionne pas sur les agents IPv6 purs.
- Les agents en ligne installent le module de protection des données immédiatement. Les agents hors ligne et itinérants installent le module dès qu'ils sont à nouveau en ligne.
- Les utilisateurs doivent redémarrer leurs ordinateurs pour finaliser l'installation des pilotes Prévention contre la perte de données. Informez les utilisateurs qu'un redémarrage anticipé est nécessaire.
- Trend Micro vous recommande d'activer la journalisation du débogage pour pouvoir résoudre les problèmes de déploiement. Pour obtenir des informations détaillées, consultez la section *Activation de la journalisation de débogage pour le module Protection des données à la page 10-63*.

Déploiement du module de protection des données sur des agents OfficeScan

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, vous pouvez :

- cliquer sur l'icône du domaine racine ( ) pour déployer le module sur tous les agents existants et à venir ;
- sélectionner un domaine spécifique pour déployer le module sur tous les agents existants et à venir qui s'y trouvent ;
- sélectionner un agent spécifique afin de déployer le module uniquement sur cet agent.

3. Déployez le module de deux manières différentes :

- Cliquez sur **Paramètres** > **Paramètres DLP**.
- Cliquez sur **Paramètres** > **Paramètres de contrôle des dispositifs**.



Remarque

Si vous procédez au déploiement à partir de **Paramètres** > **Paramètres DLP** et si le module de protection des données a été déployé avec succès, les pilotes de prévention contre la perte de données sont installés. Si les pilotes sont correctement installés, un message s'affiche, invitant les utilisateurs à redémarrer leurs endpoints afin de finaliser l'installation des pilotes.

Si le message ne s'affiche pas, il peut y avoir des problèmes pour installer les pilotes. Si vous avez activé la journalisation du débogage, vérifiez les journaux de débogage pour en savoir plus sur les problèmes relatifs à l'installation des pilotes.

4. Un message s'affiche, indiquant le nombre d'agents pour lesquels le module n'a pas été installé. Cliquez sur **Oui** pour lancer le déploiement.



Remarque

Si vous cliquez sur **Non** (ou si le module n'a pas été déployé sur un ou plusieurs agents pour un motif quelconque), le même message s'affiche lorsque vous cliquez à nouveau sur **Paramètres** > **Paramètres DLP** ou **Paramètres** > **Paramètres de contrôle des dispositifs**.

Les agents OfficeScan commencent à télécharger le module depuis le serveur.

5. Vérifiez que le module a été déployé sur les agents.

a. Dans l'arborescence des agents, sélectionnez un domaine.

b. Dans l'affichage de l'arborescence des agents, sélectionnez **Affichage de la protection des données** ou **Tout afficher**.

c. Consultez la colonne **État de la protection des données**. L'état du déploiement peut être l'un des suivants :

- **En cours d'exécution** : le module a été correctement déployé et ses fonctionnalités ont été activées.
- **Redémarrage requis** : les pilotes de prévention contre la perte de données n'ont pas été installés car les utilisateurs n'ont pas redémarré leurs ordinateurs. Si les pilotes ne sont pas installés, la prévention contre la perte de données ne pourra pas fonctionner.
- **Arrêté** : Le service du module n'a pas été démarré ou le endpoint cible a été arrêté normalement. Pour démarrer le service de protection des données, accédez à **Agents** > **Gestion des agents > Paramètres** > **Paramètres des services complémentaires** et activez les services de protection des données.
- **Ne peut pas être installé** : un problème est survenu lors du déploiement du module sur l'agent. Vous devez redéployer le module à partir de l'arborescence des agents.
- **Installation impossible (la prévention contre la perte de données existe déjà)** : Le logiciel Trend Micro Data Loss Prevention existe déjà sur le endpoint. OfficeScan ne le remplacera pas par le module de protection des données.
- **Non installé** : le module n'a pas été déployé sur l'agent. Cet état s'affiche si vous choisissez de ne pas déployer le module sur l'agent, ou si l'état de l'agent est « Hors ligne » ou « Itinérant » pendant le déploiement.

Dossier légal et base de données de prévention contre la perte de données

Lorsqu'un incident de prévention contre la perte de données se produit, OfficeScan journalise les informations de l'incident dans une base de données légale spécifique. OfficeScan crée également un fichier chiffré contenant une copie des données sensibles qui ont déclenché l'incident, puis il génère une valeur de hachage à des fins de vérification et pour garantir l'intégrité des données sensibles. OfficeScan crée les fichiers de données légales chiffrés sur l'ordinateur de l'agent et les charge ensuite sur un emplacement défini du serveur.



Important

- Les fichiers légaux chiffrés contiennent des données sensibles et les administrateurs doivent faire très attention lorsqu'ils accordent les droits d'accès à ces fichiers.
- OfficeScan s'intègre à Control Manager afin de fournir aux utilisateurs de Control Manager disposant des rôles de DLP Incident Reviewer ou de DLP Compliance Officer la possibilité d'accéder aux données des fichiers chiffrés. Pour obtenir des informations sur les rôles DLP et l'accès aux données des fichiers légaux dans Control Manager, consultez *Control Manager - Manuel de l'administrateur 6.0 Patch 2* ou version ultérieure.

Modification des paramètres du dossier légal et de la base de données légales

Les administrateurs peuvent modifier l'emplacement et la programmation de suppression du dossier légal. Ils peuvent également modifier la taille maximale des fichiers que les agents chargent en modifiant les fichiers INI d'OfficeScan.



AVERTISSEMENT!

La modification de l'emplacement du dossier légal après avoir journalisé les incidents de prévention contre la perte de données peut entraîner une déconnexion entre les données de la base de données et l'emplacement des fichiers légaux existants. Trend Micro recommande d'effectuer une migration manuelle des fichiers légaux existants vers le nouveau dossier légal après avoir modifié l'emplacement du dossier légal.

Le tableau suivant décrit les paramètres du serveur disponibles dans le fichier <*Dossier d'installation du serveur*>`\PCCSRV\Private\ofcserver.ini` qui se trouve sur le serveur OfficeScan.

TABLEAU 3-1. Paramètres du serveur du dossier légal sous `PCCSRV\Private\ofcserver.ini`

OBJECTIF	PARAMÈTRE INI	VALEURS
Activation de l'emplacement du dossier légal défini par l'utilisateur	[INI_IDLP_SECTION] `EnableUserDefinedUploadFolder`	0: Désactiver (par défaut) 1: Activer
Configuration de l'emplacement du dossier légal défini par l'utilisateur	[INI_IDLP_SECTION] `UserDefinedUploadFolder` **Remarque** • Les administrateurs doivent activer le paramètre `EnableUserDefinedUploadFolder` avant que la prévention contre la perte de données ne l'applique. • L'emplacement par défaut du dossier légal est : <*Dossier d'installation du serveur*>`\PCCSRV\Private\DLPForensicData` • L'emplacement du dossier légal défini par l'utilisateur doit être un lecteur physique (interne ou externe) sur l'ordinateur utilisé comme serveur. OfficeScan ne prend pas en charge le mappage d'un emplacement de lecteur réseau.	Valeur par défaut : <Remplacez cette valeur par le chemin d'accès du dossier défini par le client. Par exemple : C:\VolumeData\OfficeScanDlpForensicData> Valeur définie par l'utilisateur : doit être l'emplacement physique d'un lecteur sur l'ordinateur utilisé comme serveur.

Objectif	Paramètre INI	Valeurs
Activation de la purge des fichiers de données légales	[INI_IDLP_SECTION] `ForensicDataPurgeEnable`	0: Désactiver 1: Activer (par défaut)
Configuration de la fréquence de vérification de la purge du fichier de données légales	[INI_IDLP_SECTION] `ForensicDataPurgeCheckFrequency` **Remarque** • Les administrateurs doivent activer le paramètre `ForensicDataPurgeEnable` avant qu'OfficeScan ne l'applique. • OfficeScan supprime uniquement les fichiers de données qui ont dépassé la date d'expiration spécifiée par le paramètre `ForensicDataExpiredPeriodInDays`	1: tous les mois, le premier jour du mois à 00:00 2: toutes les semaines (par défaut), chaque dimanche à 00:00 3: tous les jours, chaque jour à 00:00 4: toutes les heures, chaque heure à HH:00
Configuration de la durée de stockage des fichiers de données légales sur le serveur	[INI_IDLP_SECTION] `ForensicDataExpiredPeriodInDays`	Valeur par défaut (en jours) : 180 Valeur minimale : 1 Valeur maximale : 3650

Objectif	Paramètre INI	Valeurs
Configuration de la fréquence de vérification de l'espace disque du fichier légal	[INI_SERVER_DISK_THRESHOLD] `MonitorFrequencyInSecond` **Remarque** Si l'espace disque disponible dans le dossier de données légales est inférieur à la valeur configurée dans le paramètre `InformUploadOnDiskFreeSpaceInGb`, OfficeScan enregistre un journal d'événement sur la console Web.	Valeur par défaut (en secondes) : 5
Configuration de la fréquence de chargement de vérification de l'espace disque du fichier légal	[INI_SERVER_DISK_THRESHOLD] `IsapiCheckCountInRequest` **Remarque** Si l'espace disque disponible dans le dossier de données légales est inférieur à la valeur configurée dans le paramètre `InformUploadOnDiskFreeSpaceInGb`, OfficeScan enregistre un journal d'événement sur la console Web.	Valeur par défaut (en nombre de fichiers) : 200
Configuration de la valeur minimale d'espace disque qui déclenche une notification d'espace disque restreint	[INI_SERVER_DISK_THRESHOLD] `InformUploadOnDiskFreeSpaceInGb` **Remarque** Si l'espace disque disponible dans le dossier de données légales est inférieur à la valeur configurée, OfficeScan enregistre un journal d'événement sur la console Web.	Valeur par défaut (en Go) : 10

OBJECTIF	PARAMÈTRE INI	VALEURS
Configuration de l'espace minimal disponible pour charger les fichiers de données légales depuis les agents	[INI_SERVER_DISK_THRESHOLD] `RejectUploadOnDiskFreeSpaceInGb` **Remarque** Si l'espace disque disponible dans le dossier de données légales est inférieur à la valeur configurée, les agents OfficeScan ne chargent pas les fichiers de données légales sur le serveur et OfficeScan enregistre un journal d'événement sur la console Web.	Valeur par défaut (en Go) : 1

Le tableau suivant décrit les paramètres de l'agent OfficeScan disponibles dans le fichier <*dossier d'installation du serveur*>`\PCCSRV\ofcscan.ini` qui se trouve sur le serveur OfficeScan.

TABLEAU 3-2. Paramètres de l'agent pour le fichier légal dans `PCCSRV\ofcscan.ini`

OBJECTIF	PARAMÈTRE INI	VALEURS
Activation du chargement des fichiers de données légales sur le serveur	`UploadForensicDataEnable`	0: Désactiver 1: Activer (par défaut)
Configuration de la taille maximale des fichiers que l'agent OfficeScan charge sur le serveur	`UploadForensicDataSizeLimitInMb` **Remarque** L'agent OfficeScan n'envoie vers le serveur que des fichiers dont la taille est inférieure à celle-ci.	Valeur par défaut (en Mo) : 10 Valeur minimale : 1 Valeur maximale : 2048

OBJECTIF	PARAMÈTRE INI	VALEURS
Configuration de la durée de stockage des fichiers de données légales sur l'agent OfficeScan	`ForensicDataKeepDays` **Remarque** L'agent OfficeScan supprime les fichiers de données légales qui ont dépassé la date d'expiration spécifiée chaque jour à 11h00.	Valeur par défaut (en jours) : 180 Valeur minimale : 1 Valeur maximale : 3650
Configuration de la fréquence à laquelle l'agent OfficeScan vérifie la connectivité au serveur	`ForensicDataDelayUploadFrequenceInMinutes` **Remarque** Les agents OfficeScan qui ne parviennent pas à charger automatiquement les fichiers légaux sur le serveur tentent de renvoyer les fichiers après l'intervalle de temps spécifié.	Valeur par défaut (en minutes) : 5 Valeur minimale : 5 Valeur maximale : 60

Création d'une sauvegarde des données légales

En fonction de la stratégie de sécurité de la société, la durée de stockage nécessaire des données légales peut varier énormément. Afin de libérer de l'espace disque sur le serveur, Trend Micro recommande d'effectuer une sauvegarde manuelle des données des dossiers légaux et de la base de données légales.

Procédure

1. Accédez à l'emplacement du dossier de données légales sur le serveur.
   - Emplacement par défaut : <*Dossier d'installation du serveur*>`\PCCSRV\Private\DLPForensicData`
   - Pour trouver l'emplacement du dossier légal personnalisé, consultez *Configuration de l'emplacement du dossier légal défini par l'utilisateur à la page 3-11*.
2. Copiez le dossier vers un nouvel emplacement.

3. Pour effectuer une sauvegarde manuelle de la base de données légales, accédez à <*Dossier d'installation du serveur*>`\PCCSRV\Private`.
4. Copiez le fichier `DLPForensicDataTracker.db` sur un nouvel emplacement.

Désinstallation de la protection des données

Si vous désinstallez le module de protection des données de Plug-in Manager :

- Toutes les configurations de prévention contre la perte de données, les paramètres et les journaux sont supprimés du serveur OfficeScan.
- Tous les paramètres et configurations du contrôle des dispositifs fournis par le module de protection des données sont supprimés du serveur.
- Le module de protection des données est supprimé des agents. Les endpoints des agents doivent être redémarrés pour supprimer complètement la protection des données.
- Les stratégies de prévention contre la perte de données ne seront plus appliquées sur les agents.
- Le contrôle des dispositifs ne surveille plus l'accès aux dispositifs suivants :
    - Cartes Bluetooth
    - Ports COM et LPT
    - Interface IEEE 1394
    - Périphériques d'images
    - Périphériques infrarouges
    - Modems
    - Carte PCMCIA
    - Touche Impr. écran
    - Cartes d'interface réseau sans fil

Réinstallez le module Protection des données à tout moment. Après la réinstallation, activez la licence en utilisant un code d'activation valide.

Désinstallation de la protection des données à partir de Plug-In Manager

Procédure

1. Ouvrez la console Web OfficeScan, puis cliquez sur **Modules additionnels** dans le menu principal.
2. Dans l'écran **Plug-in Manager**, accédez à la section **Protection des données OfficeScan** et cliquez sur **Désinstaller**.
3. Surveillez la progression de la désinstallation. Vous pouvez naviguer dans une autre fenêtre pendant l'opération.
4. Actualisez l'écran **Plug-in Manager** après la désinstallation. La protection des données OfficeScan peut désormais être de nouveau installée.

Partie II

Protection des agents OfficeScan



Chapitre 4

Utilisation de Trend Micro Smart Protection

Ce chapitre présente les solutions Trend Micro™ Smart Protection et explique comment configurer l'environnement requis pour les utiliser.

Les rubriques sont les suivantes :

À propos de Trend Micro Smart Protection

Trend Micro™ Smart Protection constitue une infrastructure de sécurité du contenu en ligne de nouvelle génération conçue pour protéger les clients contre les risques de sécurité et les menaces Internet. Elle repose sur des solutions à la fois locales et hébergées pour protéger les utilisateurs, qu'ils se trouvent sur le réseau, chez eux ou en voyage, à l'aide d'agents peu invasifs permettant d'accéder à une combinaison unique de technologies en ligne de messagerie, de File Reputation et de sites Web, alliées à des bases de données de menaces. La protection des clients est automatiquement mise à jour et renforcée au fur et à mesure que le nombre de produits, services et utilisateurs accédant au réseau augmente et constitue ainsi un service de protection de voisinage en temps réel pour ses utilisateurs.

Grâce à l'intégration de technologies en ligne de réputation, de scan et de corrélation, les solutions Smart Protection de Trend Micro réduisent la dépendance vis-à-vis des téléchargements de fichiers de signatures traditionnels et éliminent les temps d'attentes habituels liés aux mises à jour de postes de travail.

Le besoin d'une nouvelle solution

Dans l'approche actuelle de la gestion des menaces basées sur les fichiers, les fichiers de signatures (ou définitions) requis pour protéger un endpoint sont, pour la plupart, fournies sur la base d'une programmation. Trend Micro envoie les fichiers de signatures par lots vers les agents. À la réception d'une nouvelle mise à jour, le logiciel de protection contre les virus/programmes malveillants de l'agent recharge en mémoire ce lot de définitions de fichiers de signatures de nouveaux risques. En cas de nouveau virus/programme malveillant, ce fichier de signatures doit à nouveau être mis à jour (partiellement ou entièrement) et rechargé sur l'agent afin d'assurer la continuité de la protection.

Avec le temps, le volume des nouvelles menaces a connu une augmentation significative. Une progression du nombre de menaces quasi-exponentielle est prévue dans les années à venir. Avec un tel taux de croissance, le nombre de risques de sécurité actuellement connus sera prochainement largement dépassé. À l'avenir, le volume des risques de sécurité représentera en soi un nouveau type de risque de sécurité. Il peut avoir un impact sur les performances des serveurs et des postes de travail, l'utilisation de la bande passante du réseau et, en général, le temps nécessaire pour fournir une protection efficace (« délai de protection »).

Trend Micro a adopté une nouvelle approche dans la gestion du volume des menaces. Elle vise à protéger les utilisateurs de Trend Micro contre le risque que représente ce volume lui-même. Cet effort d'innovation tire parti d'une technologie et d'une architecture qui permettent de transférer en ligne le stockage des signatures de virus/ programmes malveillants. Trend Micro est ainsi à même de mieux protéger les clients contre le volume de nouveaux risques de sécurité.

Services Smart Protection

Smart Protection comprend des services qui fournissent des bases de données de signatures anti-programmes malveillants, de réputation de sites web et de menaces stockées en ligne.

Les services Smart protection comprennent :

- **Services de File Reputation** : Les services File Reputation transfèrent un nombre important de signatures anti-programmes malveillants auparavant stockées sur les ordinateurs d'agents vers des sources Smart Protection. Pour obtenir des informations détaillées, voir *Services de File Reputation à la page 4-3*.
- **Services de réputation de sites Web** : Les services de réputation de sites Web permettent à des sources Smart Protection locales d'héberger des données de réputation d'URL auparavant hébergées uniquement par Trend Micro. Ces deux technologies consomment moins de bande passante lors de la mise à jour des signatures ou de la vérification de la validité des URL. Pour obtenir des informations détaillées, voir *Services de réputation de sites Web à la page 4-4*.
- **Smart Feedback** : Trend Micro continue à collecter les informations envoyées anonymement du monde entier à partir de produits Trend Micro, de façon à identifier proactivement chaque nouvelle menace. Pour obtenir des informations détaillées, voir *Smart Feedback à la page 4-5*.

Services de File Reputation

Les services de File Reputation vérifient la réputation de chaque fichier par rapport à une base de données en ligne étendue. Les informations sur les programmes malveillants étant stockées en ligne, elles sont instantanément accessibles à tous les utilisateurs. Des

réseaux de transmission de contenu et des serveurs de cache très performants garantissent un temps de latence minimum pendant le processus de vérification. L'architecture de l'agent en ligne procure une protection immédiate et élimine la contrainte liée au déploiement de fichiers de signatures tout en réduisant sensiblement l'encombrement sur l'agent.

Les agents doivent être en mode Smart Scan pour pouvoir utiliser les services File Reputation. Ces agents sont appelés agents Smart Scan dans le présent document. Les agents qui ne sont pas en mode Smart Scan et qui n'ont pas recours aux services File Reputation sont appelés agents de scan traditionnel. Les administrateurs OfficeScan peuvent configurer plusieurs ou tous les agents pour qu'ils soient en mode Smart Scan.

OfficeScan doit être en mode Smart Scan pour pouvoir utiliser les services File Reputation.

Services de réputation de sites Web

Dotée de l'une des plus grandes bases de données de réputation de domaine du monde, la technologie de réputation de sites Web de Trend Micro assure le suivi de la crédibilité des domaines Web en attribuant un score de réputation dépendant de facteurs tels que l'ancienneté du site Web concerné, l'historique de ses changements d'emplacement et les indications d'activités suspectes mises en lumière par l'analyse de comportement des programmes malveillants. Les services de réputation de sites Web continuent ensuite à scanner les sites et à empêcher les utilisateurs d'accéder à ceux qui sont infectés. Les fonctionnalités de réputation de sites Web permettent de garantir que les pages consultées par les utilisateurs sont sans danger et exemptes de menaces Web, telles que les programmes malveillants, les spywares et les attaques de phishing visant à duper les utilisateurs afin de leur faire divulguer des informations personnelles. Pour une plus grande précision et une réduction des faux positifs, la technologie de réputation de sites Web de Trend Micro affecte des scores de réputation à des pages et liens spécifiques de chaque site, plutôt que de classer comme suspects des sites entiers ou de les bloquer. En effet, il arrive souvent que seule une portion d'un site légitime ait été piratée et les réputations peuvent changer de manière dynamique au fil du temps

Les agents OfficeScan soumis à des stratégies de réputation de sites Web utilisent des services de réputation de sites Web. Les administrateurs OfficeScan peuvent soumettre tous les agents ou certains d'entre eux à des stratégies de réputation de sites Web.

Smart Feedback

Trend Micro Smart Feedback assure la communication permanente entre les produits Trend Micro et les centres et technologies de recherche des menaces de la société, opérationnels 24h/24h et 7 jours/7. Chaque nouvelle menace identifiée par un contrôle de réputation de routine d'un seul client met automatiquement à jour toutes les bases de données de menaces de Trend Micro, et empêche que cette menace ne survienne à nouveau chez un autre client.

Grâce à l'analyse constante des données de menaces collectées par son vaste réseau mondial de clients et de partenaires, Trend Micro assure une protection automatique et en temps réel contre les dernières menaces, offrant ainsi une sécurité « unifiée », très semblable à une surveillance de voisinage automatisée qui implique la communauté dans la protection de chacun. La confidentialité des informations personnelles ou professionnelles d'un client est toujours protégée car les données sur les menaces qui sont collectées reposent sur la réputation de la source de communication et non sur le contenu de la communication en question.

Exemples d'informations envoyées à Trend Micro :

- les sommes de contrôles des fichiers
- les sites Web visités
- les données relatives aux fichiers, y compris, leur taille et l'adresse de leur emplacement
- les noms des fichiers exécutables

Vous pouvez interrompre à tout moment votre participation au programme depuis la console Web.



Conseil

Il n'est pas obligatoire de participer à Smart Feedback pour protéger ses ordinateurs. La participation de l'utilisateur est optionnelle et il peut y mettre fin à tout moment. Trend Micro recommande aux utilisateurs de participer à Smart Feedback afin d'assurer une meilleure protection globale à tous les clients Trend Micro.

Pour davantage d'informations à propos de Smart Protection Network, consultez :

http://fr.trendmicro.com/fr/technology/smart-protection-network/

Sources Smart Protection

Trend Micro fournit des services de File Reputation et de sites Web à OfficeScan et aux sources Smart Protection.

Les sources Smart Protection hébergent la majorité des définitions de signatures de virus/programmes malveillants dans le cadre des services de File Reputation. Les agents OfficeScan hébergent les définitions restantes. Un agent envoie des requêtes de scan aux sources Smart Protection si ses propres définitions de fichiers de signatures ne parviennent pas à déterminer la menace que présente un fichier. Les sources Smart Protection déterminent cette menace à l'aide des informations d'identification.

Les sources Smart Protection hébergent des données de réputation de sites Web disponibles uniquement via les serveurs hébergés Trend Micro dans le cadre de la fourniture des services de réputation de sites Web. L'agent envoie des requêtes de réputation de sites Web aux sources Smart Protection pour vérifier la réputation des sites Web auxquels un utilisateur tente d'accéder. L'agent compare la réputation d'un site Web à la stratégie appliquée en la matière sur le endpoint pour déterminer si l'accès au site est approuvé ou bloqué.

La source Smart Protection Server à laquelle un agent se connecte dépend de l'emplacement de l'agent. Les agents peuvent se connecter à Trend Micro Smart Protection Network ou à un serveur Smart Protection Server.

Trend Micro™ Smart Protection Network™

Trend Micro™ Smart Protection Network™ est une infrastructure de sécurité du contenu en ligne de nouvelle génération conçue pour protéger les clients contre les risques de sécurité et les menaces Internet. Il repose sur des solutions à la fois sur site et Trend Micro hébergées pour protéger les utilisateurs, qu'ils se trouvent sur le réseau, chez eux ou en voyage. Smart Protection Network utilise des agents légers pour accéder à un ensemble unique de technologies en ligne de corrélation de réputation de courrier électronique, de fichiers, de sites Web, ainsi que de bases de données de menaces. La protection des clients est automatiquement mise à jour et renforcée, au fur et à mesure

que le nombre de produits, services et utilisateurs accédant au réseau augmente, et constitue ainsi un service de protection de voisinage en temps réel pour ses utilisateurs.

Pour davantage d'informations à propos de Smart Protection Network, consultez :

http://fr.trendmicro.com/fr/technology/smart-protection-network/

Smart Protection Server

Les serveurs Smart Protection Server sont mis à la disposition des utilisateurs qui ont accès à leur réseau d'entreprise local. Les serveurs locaux localisent les services Smart Protection sur le réseau d'entreprise afin d'assurer une efficacité optimale.

Il existe deux types de serveurs Smart Protection Server :

- **Smart Protection Server intégré** : Le programme OfficeScan Setup comprend un serveur Smart Protection Server intégré qui s'installe sur le même endpoint que le serveur OfficeScan. Après l'installation, vous pouvez gérer les paramètres de ce serveur intégré à partir de la console Web d'OfficeScan. Le serveur intégré est conçu pour les déploiements de petite envergure d'OfficeScan. Pour les déploiements de plus grande envergure, le serveur Smart Protection Server autonome est requis.
- **Serveur Smart Protection Server autonome** : Un serveur Smart Protection Server autonome s'installe sur un serveur VMware ou Hyper-V. Le serveur autonome possède une console d'administration séparée et n'est pas géré depuis la console Web d'OfficeScan.

Sources Smart Protection comparées

Le tableau suivant met en évidence les différences entre Smart Protection Network et Smart Protection Server.

TABLEAU 4-1. Sources Smart Protection comparées

BASE DE COMPARAISON	SMART PROTECTION SERVER	TREND MICRO SMART PROTECTION NETWORK
Disponibilité	Disponible pour les agents internes, c'est-à-dire ceux qui répondent aux critères d'emplacement spécifiés sur la console Web OfficeScan	Disponible principalement pour les agents externes, c'est-à-dire ceux qui ne répondent pas aux critères d'emplacement spécifiés sur la console Web OfficeScan
Objet	Conçu dans le but de localiser les services Smart Protection sur le réseau d'entreprise afin d'assurer une efficacité optimale	Infrastructure Internet d'envergure mondiale visant à fournir des services Smart Protection aux agents qui ne bénéficient pas d'un accès direct à leur réseau d'entreprise
Administration	Les administrateurs OfficeScan installent et gèrent ces sources Smart Protection.	Trend Micro gère cette source.
Source de mise à jour des signatures	Trend Micro ActiveUpdate server	Trend Micro ActiveUpdate server
Protocoles de connexion des agents	HTTP et HTTPS	HTTPS

Fichiers de signatures Smart Protection

Les fichiers de signatures Smart Protection sont utilisés dans le cadre des services de File Reputation et de sites Web. Ils sont publiés par Trend Micro par l'intermédiaire du serveur Trend Micro ActiveUpdate.

Smart Scan Agent Pattern

Le fichier Smart Scan Agent Pattern est mis à jour quotidiennement. Il est téléchargé depuis la source de mise à jour des agents OfficeScan (à savoir le serveur OfficeScan ou

une source de mise à jour personnalisée). La source de mise à jour déploie ensuite le fichier de signatures sur les agents Smart Scan.



Remarque

Les agents Smart Scan sont des agents OfficeScan que les administrateurs ont configuré de façon à ce qu'ils utilisent les services File Reputation. Les agents n'ayant pas recours aux services File Reputation sont appelés agents de scan traditionnel.

Les agents Smart Scan utilisent le fichier Smart Scan Agent Pattern lors des scans ayant pour but de détecter les risques de sécurité. Si le fichier de signatures ne peut déterminer les risques impliqués par un fichier, un autre fichier de signatures, appelé Smart Scan Pattern, est appliqué.

Smart Scan Pattern

Le fichier Smart Scan Pattern est mis à jour toutes les heures. Il se télécharge à partir de sources Smart Protection. Les agents Smart Scan ne téléchargent pas le fichier Smart Scan Pattern. Les agents vérifient les menaces potentielles par rapport au fichier Smart Scan Pattern en envoyant des requêtes de scan aux sources Smart Protection.

Liste de blocage de sites Web

Les sources Smart Protection téléchargent la liste de blocage des sites. Les agents OfficeScan soumis aux stratégies de réputation de sites Web ne téléchargent pas la liste de blocage de sites Web.



Remarque

Les administrateurs peuvent soumettre tous les agents ou seulement certains d'entre eux aux stratégies de réputation de sites Web.

Les agents soumis aux stratégies de réputation de sites Web vérifient la réputation d'un site par rapport à la liste de blocage de sites Web. Pour cela, ils envoient une requête de réputation de site Web à une source Smart Protection. L'agent compare les données de réputation qu'il reçoit de la source Smart Protection à la stratégie de réputation de sites

Web en vigueur sur le endpoint. Selon la stratégie appliquée, l'agent approuve ou bloque l'accès au site.

Processus de mise à jour des signatures Smart Protection

Toutes les mises à jour de fichiers Smart Protection Pattern proviennent du serveur Trend Micro ActiveUpdate Server.

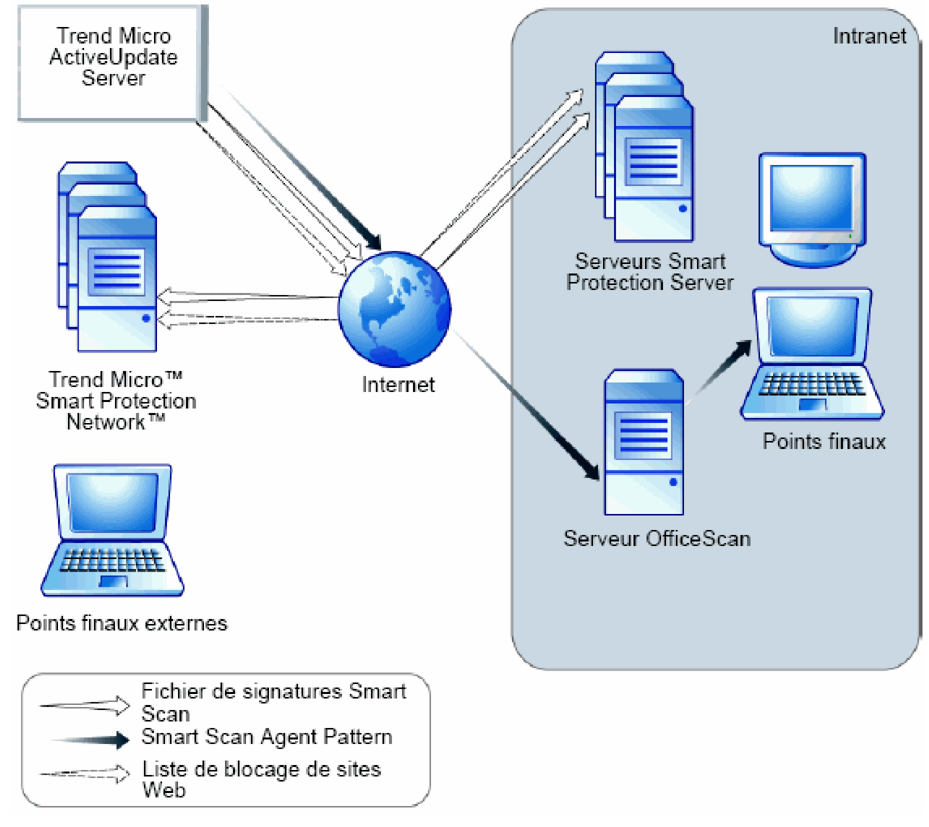


Figure 4-1. Processus de mise à jour des signatures

Utilisation des signatures Smart Protection

Un agent OfficeScan utilise le fichier Smart Scan Agent Pattern pour procéder à un scan des risques de sécurité. Il interroge uniquement le fichier Smart Scan Pattern dans le cas où le fichier Smart Scan Agent Pattern ne parvient pas à déterminer si un fichier présente une menace ou non. Lorsqu'un utilisateur tente d'accéder à un site Web, l'agent interroge la liste de blocage de sites Web. La technologie de filtre avancée permet à l'agent de « mettre en mémoire cache » les résultats de la requête. Ainsi, il n'est plus nécessaire d'envoyer plusieurs fois une seule et même question.

Les agents actuellement présents sur votre intranet peuvent se connecter à un serveur Smart Protection Server pour interroger le fichier Smart Scan Pattern ou la liste de blocage de sites Web. Une connexion réseau est requise pour se connecter au serveur Smart Protection Server. Si plusieurs serveurs Smart Protection Server ont été configurés, les administrateurs peuvent déterminer la priorité de connexion.



Conseil

Installez plusieurs serveurs Smart Protection Server pour assurer la continuité de la protection dans le cas où la connexion à un serveur Smart Protection Server n'est pas possible.

Les agents qui ne se trouvent pas sur votre intranet peuvent se connecter à Trend Micro Smart Protection Network pour envoyer des requêtes. Une connexion Internet est requise pour se connecter à Smart Protection Network.

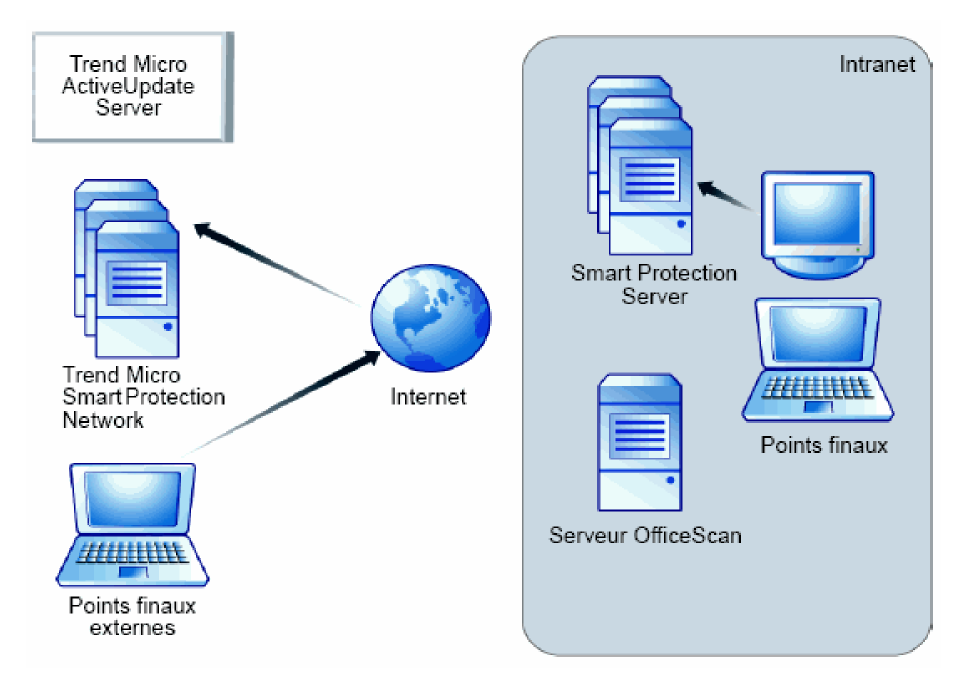


FIGURE 4-2. Processus de requête

Les agents n'ayant pas accès au réseau ou à Internet bénéficient toujours de la protection fournie par le fichier Smart Scan Agent Pattern et par la mémoire cache contenant les résultats des requêtes précédentes. La protection est réduite uniquement lorsqu'une nouvelle requête s'avère nécessaire et que l'agent ne parvient pas, en dépit de plusieurs tentatives, à joindre une source Smart Protection. Dans de tels cas, l'agent marque le fichier pour vérification et autorise temporairement l'accès au fichier. Lorsque la connexion à une source Smart Protection est restaurée, tous les fichiers marqués d'un indicateur sont scannés à nouveau. L'action de scan appropriée est ensuite effectuée sur les fichiers dont la menace a été confirmée.

Le tableau suivant récapitule la portée de la protection en fonction de l'emplacement de l'agent.

Tableau 4-2. Comportements de protection en fonction de l'emplacement

Emplacement	Fichier de signatures et comportement de requête
Accès à l'intranet	• **Fichier de signatures** : les agents téléchargent le fichier Smart Scan Agent Pattern depuis le serveur OfficeScan ou depuis une source de mise à jour personnalisée. • **Requêtes de File Reputation et de réputation de sites Web** : les agents se connectent au serveur Smart Protection Server pour les requêtes.
Sans accès à l'intranet mais avec une connexion à Smart Protection Network	• **Fichier de signatures** : les agents ne téléchargent le fichier Smart Scan Agent Pattern le plus récent que si une connexion à un serveur OfficeScan ou à une source de mise à jour personnalisée est disponible. • **Requêtes de File Reputation et de réputation de sites Web** : les agents se connectent à Smart Protection Network pour les requêtes.
Sans accès à l'intranet et sans connexion à Smart Protection Network	• **Fichier de signatures** : les agents ne téléchargent le fichier Smart Scan Agent Pattern le plus récent que si une connexion à un serveur OfficeScan ou à une source de mise à jour personnalisée est disponible. • **Requêtes de File Reputation et de réputation de sites Web** : les agents ne reçoivent pas de résultats de requête et dépendent du fichier Smart Scan Agent Pattern ainsi que de la mémoire cache contenant les résultats des requêtes précédentes.

Configuration des services Smart Protection

Avant que les agents puissent utiliser les services File Reputation et de réputation de sites Web, assurez-vous que l'environnement Smart Protection a correctement été configuré. Vérifiez ce qui suit :

- *Installation du serveur Smart Protection Server à la page 4-14*

- *Gestion du serveur Smart Protection Server intégré à la page 4-20*
- *Liste des sources Smart Protection à la page 4-26*
- *Paramètres proxy de connexion de l'agent à la page 4-33*
- *Installations de Trend Micro Network VirusWall à la page 4-34*

Installation du serveur Smart Protection Server

Vous pouvez utiliser le serveur Smart Protection Server intégré ou autonome si le nombre d'agents est inférieur à 1 000. S'il est supérieur à 1 000, installez un serveur Smart Protection Server autonome.

Trend Micro recommande que vous installiez plusieurs serveurs Smart Protection Server à des fins de basculement. Les agents ne pouvant pas se connecter à un serveur particulier tentent de se connecter aux autres serveurs que vous avez configurés.

Du fait que le serveur intégré et le serveur OfficeScan s'exécutent sur le même endpoint, les performances de ce dernier peuvent être fortement réduites pendant les pointes de trafic des deux serveurs. Pour les agents, envisagez d'utiliser un serveur Smart Protection Server autonome comme source Smart Protection principale et le serveur intégré comme source de secours.

Installation du serveur Smart Protection Server autonome

Pour obtenir des instructions sur l'installation et la gestion du serveur Smart Protection Server autonome, consultez le *Manuel d'installation et e mise à jour Trend Micro Smart Protection Server*.

Installation du serveur Smart Protection Server intégré

Si vous avez installé le serveur intégré pendant l'installation du serveur OfficeScan :

- Activez le serveur intégré et configurez les paramètres du serveur. Pour obtenir des informations détaillées, voir *Gestion du serveur Smart Protection Server intégré à la page 4-20*.
- Si le serveur intégré et l'agent OfficeScan coexistent sur le même ordinateur serveur, envisagez la désactivation du pare-feu OfficeScan. Le pare-feu OfficeScan

est conçu pour être utilisé par les endpoints des agents ; il peut affecter les performances s'il est activé sur des serveurs. Pour obtenir des instructions sur la désactivation du pare-feu, voir *Activation ou désactivation du pare-feu OfficeScan à la page 12-6*.



Remarque

Examinez les conséquences de la désactivation du pare-feu et assurez-vous qu'elle est conforme à vos plans en matière de sécurité.



Conseil

Installez Smart Protection Server intégré à la fin de l'installation d'OfficeScan en utilisant l'*Outil du serveur Smart Protection Server intégré à la page 4-15*.

Outil du serveur Smart Protection Server intégré

L'outil Smart Protection intégré d'OfficeScan de Trend Micro permet aux administrateurs d'installer ou de désinstaller un serveur Smart Protection Server intégré une fois que l'installation du serveur OfficeScan est terminée. La version actuelle d'OfficeScan ne permet pas aux administrateurs d'installer/de supprimer un serveur Smart Protection Server intégré, une fois que l'installation du serveur OfficeScan est terminée. Cet outil améliore la flexibilité des fonctionnalités d'installation par rapport aux versions précédentes d'OfficeScan.

Avant d'effectuer l'installation du serveur Smart Protection Server intégré, vous devez importer les paramètres suivants sur votre serveur OfficeScan 11.0 mis à niveau :

- Structures de domaine
- Les paramètres au niveau de la racine et du domaine :
    - Configurations de scan pour tous les types de scan (scan en temps réel, manuel, programmé et immédiat)
    - Paramètres de réputation de sites Web
    - Paramètres de surveillance des comportements
    - Paramètres de contrôle des dispositifs

    - Paramètres de prévention contre la perte de données
    - Privilèges et autres paramètres
    - Paramètres des services complémentaires
    - Liste des spywares/graywares approuvés
- Paramètres généraux de l'agent
- Emplacement de l'Endpoint
- Stratégies et profils de pare-feu
- Sources Smart Protection
- Programme de mise à jour du serveur
- Source et programme de mise à jour de l'agent
- Notifications
- Paramètres proxy

Procédure

1. Ouvrez une invite de commande et remplacez le répertoire existant par <*dossier d'installation du serveur*>`\PCCSRV\`Admin\Utility\ISPSInstaller, répertoire dans lequel se trouve `ISPSInstaller.exe`.

2. Exécutez `ISPSInstaller.exe` à l'aide de l'une des commandes suivantes :

Tableau 4-3. Options du programme d'installation.

Commande	Description
`ISPSInstaller.exe /i`	Installe le serveur Smart Protection Server intégré en utilisant les paramètres de port par défaut. Pour plus de détails sur les paramètres de port par défaut, reportez-vous au tableau ci-dessous.

Commande	Description
`ISPSInstaller.exe /i /f:[numéro de port] /s:[numéro de port] /w:[numéro de port]`	Installe le serveur intégré Smart Protection Server en utilisant les ports spécifiés, sur lesquels : • `/f:[numéro de port]` représente le port HTTP file reputation • `/s:[numéro de port]` représente le port HTTPS file reputation • `/w:[numéro de port]` représente le port de réputation de sites Web **Remarque** Une valeur par défaut est automatiquement attribuée au port non spécifié.
`ISPSInstaller.exe /u`	Désinstalle le serveur intégré Smart Protection Server

Tableau 4-4. Ports pour les services de réputation de sites Web du serveur Smart Protection Server intégré

Serveur Web et paramètres	Ports pour les services de File Reputation		Port HTTP pour les services de réputation de sites Web
	HTTP	HTTPS (SSL)	
Serveur Web Apache sur lequel SSL est activé	8082	4345 (non configurable)	5274 (non configurable)
Serveur Web Apache sur lequel SSL est désactivé	8082	4345 (non configurable)	5274 (non configurable)
Site Web par défaut IIS sur lequel SSL est activé	80	443 (non configurable)	80 (non configurable)
Site Web par défaut IIS sur lequel SSL est désactivé	80	443 (non configurable)	80 (non configurable)

Serveur Web et paramètres	Ports pour les services de File Reputation		Port HTTP pour les services de réputation de sites Web
	HTTP	HTTPS (SSL)	
Site Web virtuel IIS sur lequel SSL est activé	8080	4343 (configurable)	8080 (configurable)
Site Web virtuel IIS sur lequel SSL est désactivé	8080	4343 (configurable)	8080 (configurable)

3. Une fois que l'installation est terminée, ouvrez la console Web OfficeScan et vérifiez les informations suivantes :

- Ouvrez la console d'administration **Microsoft Management Console** (en saisissant `services.msc` dans le menu **Démarrer**) et assurez-vous que Trend Micro Local Web Classification Server et Trend Micro Smart Scan Server indiquent l'état « Démarré » dans la liste.
- Ouvrez le **Gestionnaire des tâches Windows**. Dans l'onglet **Processus**, vérifiez que `iCRCService.exe` et `LWCSService.exe` sont en cours d'exécution,
- Sur la console Web OfficeScan, vérifiez que l'option de menu **Administration** > **Smart Protection** > **Serveur intégré** est bien affichée.

Pratiques recommandées relatives au serveur Smart Protection Server

Optimisez les performances des serveurs Smart Protection Server en exécutant les tâches suivantes :

- Évitez d’effectuer un scan manuel et un scan programmé simultanément. Échelonnez les scans par groupes.
- Configurez les agents de manière à éviter qu'ils effectuent un scan immédiat simultanément.

- Personnalisez les serveurs Smart Protection Server pour les connexions réseau lentes (environ 512 Kbits/s) en effectuant les modifications suivantes dans le fichier `ptngrowth.ini`.

Personnalisation du fichier « ptngrowth.ini » pour le serveur autonome

Procédure

1. Ouvrez le fichier `ptngrowth.ini` dans `/var/tmcss/conf/`.
2. Modifiez le fichier `ptngrowth.ini` file en utilisant les valeurs recommandées suivantes :
   - `[COOLDOWN]`
   - `ENABLE=1`
   - `MAX_UPDATE_CONNECTION=1`
   - `UPDATE_WAIT_SECOND=360`
3. Enregistrez le fichier `ptngrowth.ini`.
4. Redémarrez le service `lighttpd` en saisissant la commande suivante dans l'interface de ligne de commande (CLI) :
   - `redémarrge du service lighttpd`

Personnalisation du fichier « ptngrowth.ini » pour le serveur intégré

Procédure

1. Ouvrez le fichier `ptngrowth.ini` qui se trouve dans le répertoire <*dossier d'installation du serveur*>`\PCCSRV\WSS\`.
2. Modifiez le fichier `ptngrowth.ini` file en utilisant les valeurs recommandées suivantes :

- `[COOLDOWN]`
- `ENABLE=1`
- `MAX_UPDATE_CONNECTION=1`
- `UPDATE_WAIT_SECOND=360`

3. Enregistrez le fichier `ptngrowth.ini`.

4. Redémarrez le service `Trend Micro Smart Protection Server`.

Gestion du serveur Smart Protection Server intégré

Gérez le serveur Smart Protection Server intégré à l'aide des tâches suivantes :

- Activation des services de File Reputation et des services de réputation de sites Web du serveur intégré
- enregistrement des adresses du serveur intégré
- mise à jour des composants du serveur intégré
- configuration de la liste des URL approuvées/bloquées du serveur intégré.
- Configuration des paramètres de liste de Virtual Analyzer C&C

Pour obtenir des informations détaillées, voir *Configuration des paramètres du serveur Smart Protection Server intégré à la page 4-23*.

Activation des services de File Reputation et des services de réputation de sites Web du serveur intégré

Pour que les agents puissent envoyer des requêtes de scan et de réputation de sites Web au serveur intégré, les services File Reputation et les services de réputation de sites Web doivent être activés. L'activation de ces services permet également au serveur intégré de mettre à jour les composants à partir du serveur ActiveUpdate.

Ces services sont automatiquement activés si vous avez choisi d'installer le serveur intégré pendant l'installation du serveur OfficeScan Server.

Si vous désactivez ces services, assurez-vous d'avoir installé des serveurs Smart Protection Server autonomes auxquels les agents peuvent envoyer des requêtes.

Pour obtenir des informations détaillées, voir *Configuration des paramètres du serveur Smart Protection Server intégré à la page 4-23*.

Enregistrement des adresses du serveur intégré

Pour configurer la liste des sources Smart Protection pour les agents internes, vous aurez besoin des adresses du serveur intégré. Pour plus de détails sur la liste, voir *Liste des sources Smart Protection à la page 4-26*.

Lorsque des agents envoient des requêtes de scan au serveur intégré, ils identifient le serveur par l'une des deux adresses des services File Reputation : l'adresse HTTP ou l'adresse HTTPS. Une connexion avec l'adresse HTTPS est plus sécurisée, tandis qu'une connexion avec l'adresse HTTP utilise moins de bande passante.

Lorsque les agents envoient des requêtes de réputation de sites Web, ils identifient le serveur intégré par son adresse de services de réputation de sites Web.



Conseil

Les agents gérés par un autre serveur OfficeScan peuvent également se connecter à ce serveur intégré. Sur l'autre console Web du serveur OfficeScan, ajoutez l'adresse du serveur intégré à la liste des sources Smart Protection.

Pour obtenir des informations détaillées, voir *Configuration des paramètres du serveur Smart Protection Server intégré à la page 4-23*.

Mise à jour des composants du serveur intégré

Le serveur intégré met à jour les composants suivants :

- **Smart Scan Pattern** : Les agents OfficeScan vérifient les menaces potentielles par rapport au fichier Smart Scan Pattern en envoyant des requêtes de scan au serveur intégré.
- **Liste de blocage de sites Web** : les agents OfficeScan soumis aux stratégies de réputation de sites Web vérifient la réputation d'un site par rapport à la Liste de

blocage de sites Web. Pour cela, ils envoient une requête de réputation au serveur intégré.

Mettez manuellement à jour ces composants ou configurez un programme de mise à jour. Le serveur intégré télécharge les composants depuis le serveur ActiveUpdate.



Remarque

Un serveur intégré IPv6 pur ne peut pas directement faire une mise à jour à partir du serveur Trend Micro ActiveUpdate Server. Un serveur proxy double-pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre au serveur intégré de se connecter au serveur ActiveUpdate.

Pour obtenir des informations détaillées, voir *Configuration des paramètres du serveur Smart Protection Server intégré à la page 4-23*.

Configuration de la liste des URL approuvées/bloquées du serveur intégré

Les agents disposent de leur propre liste des URL approuvées/bloquées. Configurez la liste des agents lorsque vous mettez en place des stratégies de réputation de sites Web (voir *Stratégies de réputation de sites Web à la page 11-5* pour plus d'informations). Toute URL figurant dans la liste d'un agent est automatiquement approuvée ou bloquée.

Le serveur intégré dispose de sa propre liste d'URL approuvées ou bloquées. Si une URL ne figure pas dans la liste d'un agent, celui-ci envoie une requête de réputation de sites Web au serveur intégré (si le serveur intégré fait partie des sources Smart Protection). Si l'URL figure dans la liste des URL approuvées/bloquées du serveur intégré, celui-ci indique à l'agent s'il doit approuver ou bloquer l'URL.



Remarque

La liste des URL bloquées a une priorité plus élevée que la liste de blocage de sites Web.

Pour ajouter des URL à la liste des URL approuvées/bloquées du serveur intégré, importez une liste depuis un serveur Smart Protection Server autonome. Vous ne pouvez pas ajouter d'URL manuellement.

Pour obtenir des informations détaillées, voir *Configuration des paramètres du serveur Smart Protection Server intégré à la page 4-23*.

Paramètres de connexion de Deep Discovery Advisor et Virtual Analyzer

Configurez les paramètres de liste de Virtual Analyzer C&C afin d'établir une connexion entre le serveur Smart Protection Server intégré et le serveur Deep Discovery Advisor. L'analyseur virtuel de Deep Discovery Advisor crée la liste de Virtual Analyzer C&C que le serveur Smart Protection Server stocke afin qu'elle puisse être utilisée par OfficeScan.

Après avoir établi une connexion avec le serveur Deep Discovery Advisor, activez la liste Virtual Analyzer C&C pour surveiller les rappels C&C réalisés auprès serveurs précédemment identifiés par d'autres agents sur le réseau.

Pour obtenir des informations détaillées, voir *Configuration des paramètres du serveur Smart Protection Server intégré à la page 4-23*.

Configuration des paramètres du serveur Smart Protection Server intégré

Procédure

1. Accédez à **Administration** > **Smart Protection** > **Serveur intégré**.
2. Sélectionnez **Activer le service de réputation de fichiers**.
3. Sélectionnez le protocole (HTTP ou HTTPS) utilisé par les agents pour envoyer des requêtes de scan au serveur intégré.
4. Sélectionnez **Activer les services de réputation de sites Web**.
5. Enregistrez les adresses du serveur intégré dans la colonne **Adresse du serveur**.
6. Pour mettre à jour les composants du serveur intégré :
   - Consultez les versions actuelles du fichier Smart Scan Pattern et de la liste de blocage de sites Web. Si une mise à jour est disponible, cliquez sur **Mettre à jour**. Le résultat de la mise à jour s'affiche dans la partie supérieure de l'écran.

- Pour mettre automatiquement à jour le fichier de signatures :

    a. Sélectionnez **Activer les mises à jour programmées**.

    b. Indiquez si la mise à jour doit avoir lieu toutes les heures ou toutes les 15 minutes.

    c. Dans **Services de File Reputation**, sélectionnez une source de mise à jour. Le fichier Smart Scan Pattern sera mis à jour à partir de cette source.

    d. Dans **Services de réputation de sites Web**, sélectionnez une source de mise à jour. La liste de blocage de sites Web sera mise à jour à partir de cette source.



Remarque

- Si vous choisissez le serveur ActiveUpdate comme source de mise à jour, assurez-vous qu'il dispose d'une connexion Internet et, si vous utilisez un serveur proxy, testez la connexion Internet pour voir si elle peut être établie en utilisant les paramètres du proxy. Voir *Proxy for OfficeScan Server Updates à la page 6-22* pour plus d'informations.

- Si vous choisissez une source de mise à jour personnalisée, définissez l'environnement approprié et mettez à jour les ressources de cette source de mise à jour. Assurez-vous également qu'il existe une connexion opérationnelle entre le serveur et cette source de mise à jour. Si vous avez besoin d'aide pour définir une source de mise à jour, contactez votre service d'assistance.

7. Pour configurer la liste des URL approuvées/bloquées du serveur intégré :

  a. Cliquez sur **Importer** pour compléter la liste à l'aide d'URL provenant d'un fichier `.csv` préformaté. Vous pouvez obtenir le fichier `.csv` à partir d'un serveur Smart Protection Server autonome.

  b. Si vous disposez d'une liste existante, cliquez sur **Exporter** pour enregistrer la liste dans un fichier `.csv`.

8. 

Remarque

- Contactez l'administrateur de Deep Discovery Advisor pour obtenir le nom ou l'adresse IP du serveur, le numéro de port et une clé API valide.
- Cette version d'OfficeScan prend uniquement en charge Deep Discovery Advisor 3.0 et versions ultérieures.

Pour configurer la connexion Virtual Analyzer au serveur Deep Discovery Advisor :

a. Saisissez le nom ou l'adresse IP du serveur Deep Discovery Advisor.



Remarque

Le nom du serveur prend en charge les formats de noms de domaines complets (FQDN) et l'adresse IP prend en charge le format IPv4. L'adresse du serveur prend uniquement en charge le protocole HTTPS.

b. Saisissez la clé API.

c. Cliquez sur **Enregistrer** pour vous connecter au serveur Deep Discovery Advisor.



Remarque

Les administrateurs peuvent tester la connexion au serveur avant de s'enregistrer sur le serveur.

d. Sélectionnez **Activer la liste de Virtual Analyzer C&C** pour permettre à OfficeScan d'utiliser la liste C&C personnalisée analysée par le serveur Deep Discovery Advisor local.



Remarque

L'option **Activer la liste de Virtual Analyzer C&C** n'est disponible qu'après avoir correctement établi une connexion au serveur Deep Discovery Advisor.

Les administrateurs peuvent effectuer la synchronisation manuelle à Deep Discovery Advisor à tout moment en cliquant sur le bouton **Synchroniser maintenant**.

9. Cliquez sur **Enregistrer**.

Liste des sources Smart Protection

Les agents envoient des requêtes aux sources Smart Protection dans le cadre du scan des risques de sécurité et de la détermination de la réputation d'un site Web.

Prise en charge d'IPv6 pour les sources Smart Protection

Un agent IPv6 pur ne peut pas envoyer directement de requêtes à des sources IPv4 pures, telles que :

- Smart Protection Server 2.0 (intégré ou autonome)



Remarque

IPv6 est pris en charge pour le serveur Smart Protection Server à partir de la version 2.5.

- Trend Micro Smart Protection Network

De même, un agent IPv4 pur ne peut pas envoyer de requêtes à des serveurs Smart Protection IPv6 purs.

Un serveur proxy à double pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre aux agents de se connecter aux sources.

Sources Smart Protection et emplacement de l'endpoint

La source Smart Protection Server à laquelle un agent se connecte dépend de l'emplacement de l'endpoint de l'agent.

Pour obtenir des informations détaillées sur la configuration des paramètres d'emplacement, voir *Emplacement de l'Endpoint à la page 14-2*.

TABLEAU 4-5. Sources Smart Protection par emplacement

EMPLACEMENT	SOURCES SMART PROTECTION
Externe	Les agents externes peuvent envoyer des requêtes de scan et de réputation de sites Web à Trend Micro Smart Protection Network.
Interne	Les agents internes peuvent envoyer des requêtes de scan et de réputation de sites Web aux serveurs Smart Protection Server ou à Trend Micro Smart Protection Network. Si vous avez installé des serveurs Smart Protection Server, configurez la liste des sources Smart Protection sur OfficeScan web console. Un agent interne sélectionne un serveur de la liste lorsqu'il doit émettre une requête. S'il ne parvient pas à se connecter au premier serveur, il en sélectionne un autre dans la liste. **Conseil** Affectez un serveur Smart Protection Server autonome comme source de scan principale et le serveur intégré comme source de secours. Cela réduit le trafic de requêtes adressées au endpoint qui héberge le serveur OfficeScan et le serveur intégré. Le serveur autonome peut également traiter plus de requêtes. Vous pouvez configurer une liste standard ou personnalisée de sources Smart Protection. La liste standard est utilisée par tous les agents internes. Une liste personnalisée définit une plage d'adresses IP. Si l'adresse IP d'un agent interne figure dans cette plage, cet agent utilise la liste personnalisée.

Configuration de la liste standard des sources Smart Protection

Procédure

1. Accédez à **Administration** > **Smart Protection** > **Sources Smart Protection**.
2. Cliquez sur l'onglet **Agents internes**.
3. Sélectionnez **Utiliser la liste standard (pour tous les agents internes)**.
4. Cliquez sur le lien **Liste standard**.

Un nouvel écran s'affiche.

5. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.

6. Indiquez le nom d'hôte ou l'adresse IPv4/IPv6 du serveur Smart Protection. Si vous spécifiez une adresse IPv6, placez-la entre parenthèses.



Remarque

Indiquez le nom de l'hôte si des agents IPv4 et IPv6 se connectent au serveur Smart Protection Server.

7. Sélectionnez Services de File Reputation. Les agents envoient leurs requêtes de scan à l'aide du protocole HTTP ou HTTPS. HTTPS permet une connexion plus sécurisée, tandis que HTTP utilise moins de bande passante.

   a. Si vous souhaitez que les agents utilisent le protocole HTTP, saisissez le port d'écoute du serveur pour les requêtes HTTP. Si vous souhaitez que les agents utilisent le protocole HTTPS, sélectionnez SSL et saisissez le port d'écoute du serveur pour les requêtes HTTPS.

   b. Cliquez sur **Tester la connexion** pour vérifier si la connexion au serveur peut être établie.



Conseil

Les ports d'écoute font partie de l'adresse du serveur. Pour obtenir l'adresse du serveur :

Pour le serveur intégré, ouvrez la console Web OfficeScan et accédez à **Administration** > **Smart Protection** > **Serveur intégré**.

Pour le serveur autonome, ouvrez la console du serveur autonome et accédez à l'écran **Résumé**.

8. Sélectionnez **Services de réputation de sites Web**. Les agents envoient leurs requêtes de réputation de sites Web à l'aide du protocole HTTP. Le protocole HTTPS n'est pas pris en charge.

   a. Entrez le port d'écoute du serveur pour les requêtes HTTP.

b. Cliquez sur **Tester la connexion** pour vérifier si la connexion au serveur peut être établie.

9. Cliquez sur **Enregistrer**.

L'écran se ferme.

10. Répétez les étapes précédentes pour ajouter d'autres serveurs.

11. En haut de l'écran, sélectionnez **Ordre** ou **Aléatoire**.

- **Ordre** : les agents sélectionnent les serveurs dans l'ordre selon lequel ils apparaissent dans la liste. Si vous sélectionnez **Ordre**, utilisez les flèches sous la colonne **Ordre** pour déplacer les serveurs vers le haut ou le bas de la liste.
- **Aléatoire** : les agents sélectionnent des serveurs de façon aléatoire.



Conseil

Du fait que le serveur Smart Protection Server intégré et le serveur OfficeScan s'exécutent sur le même endpoint, les performances de ce dernier peuvent être fortement réduites pendant les pointes de trafic des deux serveurs. Pour réduire le trafic dirigé vers l'ordinateur du serveur OfficeScan, affectez un serveur Smart Protection Server autonome comme source Smart Protection principale, et le serveur intégré comme source de secours.

12. Exécutez des tâches diverses présentées à l'écran.

- Si vous avez exporté une liste à partir d'un autre serveur et souhaitez l'importer dans cet écran, cliquez sur **Importer** et localisez le fichier `.dat`. La liste est chargée à l'écran.
- Pour exporter la liste dans un fichier `.dat`, cliquez sur **Exporter**, puis sur **Enregistrer**.
- Pour actualiser l'état de service des serveurs, cliquez sur **Actualiser**.
- Cliquez sur le nom du serveur pour effectuer l'une des opérations suivantes :
  - Afficher ou modifier les informations sur le serveur.
  - Afficher l'adresse complète du serveur pour les services de réputation de sites Web ou de fichiers.

- Pour ouvrir la console pour un serveur Smart Protection Server, cliquez sur **Lancer la console**.
  - Pour le serveur Smart Protection Server intégré, l'écran de configuration du serveur s'affiche.
  - Pour les serveurs Smart Protection Server autonomes et le serveur Smart Protection Server intégré d'un autre serveur OfficeScan, l'écran de connexion à la console s'affiche.
- Pour supprimer une entrée, activez la case à cocher du serveur, puis cliquez sur **Supprimer**.

13. Cliquez sur **Enregistrer**.

    L'écran se ferme.

14. Cliquez sur **Notifier tous les agents**.

Configuration des listes personnalisées des sources Smart Protection

---

Procédure

1. Accédez à **Administration** > **Smart Protection** > **Sources Smart Protection**.
2. Cliquez sur l'onglet **Agents internes**.
3. Sélectionnez **Utiliser les listes personnalisées selon l'adresse IP de l'agent**.
4. (Facultatif) Sélectionnez **Utilisez la liste standard lorsqu'aucun serveur des listes personnalisées n'est disponible**.
5. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.

6. Dans la section **Plage IP**, spécifiez une plage d'adresses IPv4 ou IPv6, ou les deux.



Remarque

Les agents ayant une adresse IPv4 peuvent se connecter à des serveurs Smart Protection Server IPv4 purs ou à double pile. Les agents ayant une adresse IPv6 peuvent se connecter à des serveurs Smart Protection Server IPv6 purs ou à double pile. Les agents ayant à la fois une adresse IPv4 et une adresse IPv6 peuvent se connecter à n'importe quel serveur Smart Protection Server.

7. Dans la section **Paramètres proxy**, indiquez les paramètres proxy utilisés par les agents pour se connecter aux serveurs Smart Protection Server.

   a. Sélectionnez **Utiliser un serveur proxy pour la communication entre l'agent et le serveur Smart Protection Server**.

   b. Indiquez le nom ou l'adresse IPv4/IPv6 et le numéro de port du serveur proxy.

   c. Si le serveur proxy nécessite une authentification, tapez le nom d'utilisateur et le mot de passe appropriés.

8. Dans la **Liste des serveurs Smart Protection Server personnalisée**, ajoutez les serveurs Smart Protection Server.

   a. Indiquez le nom d'hôte ou l'adresse IPv4/IPv6 du serveur Smart Protection. Si vous spécifiez une adresse IPv6, placez-la entre parenthèses.

      Remarque

      Indiquez le nom de l'hôte si des agents IPv4 et IPv6 se connectent au serveur Smart Protection Server.

   b. Sélectionnez **Services de File Reputation**. Les agents envoient leurs requêtes de scan à l'aide du protocole HTTP ou HTTPS. HTTPS permet une connexion plus sécurisée, tandis que HTTP utilise moins de bande passante.

      i. Si vous souhaitez que les agents utilisent le protocole HTTP, saisissez le port d'écoute du serveur pour les requêtes HTTP. Si vous souhaitez que les agents utilisent le protocole HTTPS, sélectionnez **SSL** et saisissez le port d'écoute du serveur pour les requêtes HTTPS.

      ii. Cliquez sur **Tester la connexion** pour vérifier si la connexion au serveur peut être établie.



Conseil

Les ports d'écoute font partie de l'adresse du serveur. Pour obtenir l'adresse du serveur :

Pour le serveur intégré, ouvrez la console Web OfficeScan et accédez à **Administration** > **Smart Protection** > **Serveur intégré**.

Pour le serveur autonome, ouvrez la console du serveur autonome et accédez à l'écran Résumé.

c. Sélectionnez **Services de réputation de sites Web**. Les agents envoient leurs requêtes de réputation de sites Web à l'aide du protocole HTTP. Le protocole HTTPS n'est pas pris en charge.

   i. Entrez le port d'écoute du serveur pour les requêtes HTTP.

   ii. Cliquez sur **Tester la connexion** pour vérifier si la connexion au serveur peut être établie.

d. Cliquez sur **Ajouter à la liste**.

e. Répétez les étapes précédentes pour ajouter d'autres serveurs.

f. Sélectionnez **Ordre** ou **Aléatoire**.

   - **Ordre** : les agents sélectionnent les serveurs dans l'ordre selon lequel ils apparaissent dans la liste. Si vous sélectionnez **Ordre**, utilisez les flèches sous la colonne **Ordre** pour déplacer les serveurs vers le haut ou le bas de la liste.

   - **Aléatoire** : les agents sélectionnent des serveurs de façon aléatoire.



Conseil

Du fait que le serveur Smart Protection Server intégré et le serveur OfficeScan s'exécutent sur le même ordinateur, les performances de ce dernier peuvent être fortement réduites pendant les pointes de trafic des deux serveurs. Pour réduire le trafic dirigé vers l'ordinateur du serveur OfficeScan, affectez un serveur Smart Protection Server autonome comme source Smart Protection principale, et le serveur intégré comme source de secours.

g. Exécutez des tâches diverses présentées à l'écran.

- Pour actualiser l'état de service des serveurs, cliquez sur **Actualiser**.
- Pour ouvrir la console pour un serveur Smart Protection Server, cliquez sur **Lancer la console**.
    - Pour le serveur Smart Protection Server intégré, l'écran de configuration du serveur s'affiche.
    - Pour les serveurs Smart Protection Server autonomes et le serveur Smart Protection Server intégré d'un autre serveur OfficeScan, l'écran de connexion à la console s'affiche.
- Pour supprimer une entrée, cliquez sur **Supprimer** (Supprimer).

9. Cliquez sur **Enregistrer**.

L'écran se ferme. La liste que vous venez d'ajouter s'affiche sous forme de lien de plage IP sous le tableau **Plage IP**.

10. Répétez les étapes 4 à 8 pour ajouter d'autres listes personnalisées.

11. Exécutez des tâches diverses présentées à l'écran.

- Pour modifier une liste, cliquez sur le lien de la plage IP, puis modifiez les paramètres dans l'écran qui s'ouvre.
- Pour exporter la liste dans un fichier .dat, cliquez sur **Exporter**, puis sur **Enregistrer**.
- Si vous avez exporté une liste à partir d'un autre serveur et souhaitez l'importer dans cet écran, cliquez sur **Importer** et localisez le fichier `.dat`. La liste est chargée à l'écran.

12. Cliquez sur **Notifier tous les agents**.

Paramètres proxy de connexion de l'agent

Si la connexion à Smart Protection Network nécessite l'authentification proxy, indiquez les informations d'authentification. Pour obtenir des informations détaillées, voir *Proxy externe pour les agents OfficeScan à la page 14-52*.

Configurez les paramètres proxy internes que les agents utiliseront pour se connecter à un serveur Smart Protection Server. Pour obtenir des informations détaillées, voir *Proxy interne pour les agents OfficeScan à la page 14-51*.

Paramètres d'emplacement des endpoints

OfficeScan comporte une fonction de détection d'emplacement qui identifie l'emplacement de l'ordinateur de l'agent et détermine si l'agent se connecte à Smart Protection Network ou à un serveur Smart Protection Server. Cela garantit le maintien de la protection des agents quel que soit leur emplacement.

Pour configurer les paramètres d'emplacement, voir *Emplacement de l'Endpoint à la page 14-2*.

Installations de Trend Micro Network VirusWall

Si Trend Micro™ Network VirusWall™ Enforcer est installé :

- Installez un correctif de type hot fix (compilation 1047 pour Network VirusWall Enforcer 2500 et compilation 1013 pour Network VirusWall Enforcer 1200).
- Mettez à jour le moteur OPSWAT vers la version 2.5.1017 pour permettre au produit de détecter la méthode de scan d'un agent.

Utilisation des services Smart Protection

Une fois l'environnement Smart Protection correctement configuré, les agents sont prêts à utiliser les services File Reputation et de réputation de sites Web. Vous pouvez commencer à configurer les paramètres de Smart Feedback.



Remarque

Pour obtenir des instructions sur la configuration de l'environnement Smart Protection, voir *Configuration des services Smart Protection à la page 4-13*.

Afin de bénéficier de la protection fournie par les services File Reputation, les agents doivent utiliser la méthode de scan appelée Smart Scan. Pour plus d'informations sur Smart Scan et son activation sur les agents, voir *Types de méthodes de scan à la page 7-9*.

Pour autoriser les agents OfficeScan à utiliser les services de réputation de sites Web, configurez des stratégies de réputation de sites Web. Pour obtenir des informations détaillées, voir *Stratégies de réputation de sites Web à la page 11-5*.



Remarque

Les paramètres des méthodes de scan et des stratégies de réputation de sites Web sont détaillés. En fonction de vos exigences, vous pouvez configurer des paramètres qui s'appliqueront à tous les agents, ou configurer des paramètres différents pour chaque agent ou groupe d'agents.

Pour obtenir des instructions sur la configuration de Smart Feedback, voir *Smart Feedback à la page 13-61*.



Chapitre 5

Installation de l'agent OfficeScan

Ce chapitre décrit la configuration requise de Trend Micro™ OfficeScan™ et les procédures d'installation de l'agent OfficeScan.

Pour obtenir des instructions détaillées sur la mise à niveau d'un agent OfficeScan, reportez-vous au *Guide d'installation et de mise à niveau d'OfficeScan*.

Les rubriques sont les suivantes :

Nouvelles installations de l'agent OfficeScan

L'agent OfficeScan peut être installé sur des ordinateurs exécutant les plates-formes Microsoft Windows. OfficeScan est également compatible avec de nombreux produits tiers.

Visitez le site Web suivant pour obtenir la liste complète des configurations requises et des produits tiers compatibles :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Remarques relatives à l'installation

Avant d'installer des agents, tenez compte des éléments suivants :

Tableau 5-1. Éléments à prendre en compte pour l'installation d'un agent

Éléments à prendre en compte	Description
prise en charge des fonctionnalités sous Windows	Certaines fonctionnalités de l'agent OfficeScan ne sont pas disponibles sur certaines plates-formes Windows.
Prise en charge d'IPv6	L'agent OfficeScan peut être installé sur des agents IPv6 purs ou à double pile. Cependant : • Certains systèmes d'exploitation Windows sur lesquels l'agent OfficeScan peut être installé ne prennent pas en charge l'adressage IPv6. • Pour certaines méthodes d'installation, il existe des spécifications particulières à respecter pour garantir l'installation correcte de l'agent OfficeScan.
Adresses IP de l'agent OfficeScan	Pour les agents utilisant à la fois les adressages IPv4 et IPv6, vous pouvez choisir quelle adresse IP sera utilisée lors de l'enregistrement de l'agent auprès du serveur.

ÉLÉMENTS À PRENDRE EN COMPTE	DESCRIPTION
Listes des exceptions	Assurez-vous que les listes d'exceptions pour les fonctionnalités suivantes ont été configurées correctement : • **Surveillance des comportements** : ajoutez les applications nécessaires au endpoint dans la liste des programmes approuvés pour empêcher l'agent OfficeScan de bloquer ces applications. Pour plus d'informations, voir *Liste d'exceptions de la surveillance des comportements à la page 8-6*. • **Réputation de sites Web** : ajoutez les sites Web que vous considérez sans danger à la liste des URL approuvées pour empêcher l'agent OfficeScan de bloquer l'accès à ces sites Web. Pour plus d'informations, voir *Stratégies de réputation de sites Web à la page 11-5*.

Fonctionnalités de l'agent OfficeScan

Les fonctionnalités de l'agent OfficeScan disponibles sur un endpoint dépendent du système d'exploitation de ce dernier.

TABLEAU 5-2. Fonctionnalités de l'agent OfficeScan sur les plates-formes serveur

FONCTION	SYSTÈME D'EXPLOITATION WINDOWS		
	SERVER 2003	SERVER 2008/ SERVER CORE 2008	SERVER 2012/ SERVER CORE 2012
Scan manuel, scan en temps réel et scan programmé	Oui	Oui	Oui
Mise à jour des composants (mise à jour manuelle et programmée)	Oui	Oui	Oui
Agent de mise à jour	Oui	Oui	Oui

Fonction	Système d'exploitation Windows		
	Server 2003	Server 2008/ Server Core 2008	Server 2012/ Server Core 2012
Réputation de sites Web	Oui mais désactivé par défaut lors de l'installation du serveur	Oui mais désactivé par défaut lors de l'installation du serveur	Oui mais désactivé par défaut lors de l'installation du serveur et prise en charge limitée en mode Windows UI
Damage Cleanup Services	Oui	Oui	Oui
Pare-feu OfficeScan	Oui mais désactivé par défaut lors de l'installation du serveur	Oui mais désactivé par défaut lors de l'installation du serveur	Oui mais désactivé par défaut lors de l'installation du serveur et le filtrage d'applications n'est pas pris en charge
Surveillance des comportements	Oui (32 bits) mais désactivé par défaut	Oui (32 bits) mais désactivé par défaut	Oui (64 bits) mais désactivé par défaut
	Non (64 bits)	Oui (64 bits) mais désactivé par défaut	
Autoprotection de l'agent pour : • Clés de registre • Processus	Oui (32 bits) mais désactivé par défaut	Oui (32 bits) mais désactivé par défaut	Oui (64 bits) mais désactivé par défaut
	Non (64 bits)	Oui (64 bits) mais désactivé par défaut	

Fonction	Système d'exploitation Windows		
	Server 2003	Server 2008/ Server Core 2008	Server 2012/ Server Core 2012
Autoprotection de l'agent pour : • Services • Protection des fichiers	Oui	Oui	Oui
Contrôle des dispositifs (Service de prévention des modifications non autorisées)	Oui (32 bits) mais désactivé par défaut	Oui (32 bits) mais désactivé par défaut	Oui (64 bits) mais désactivé par défaut
	Non (64 bits)	Oui (64 bits) mais désactivé par défaut	
Protection des données (y compris la fonction de protection des données du contrôle des dispositifs)	Oui (32 bits) mais désactivé par défaut	Oui (32 bits) mais désactivé par défaut	Oui (64 bits) mais désactivé par défaut
	Oui (64 bits) mais désactivé par défaut	Oui (64 bits) mais désactivé par défaut	
Scan de la messagerie POP3	Oui	Oui	Oui
Plug-in Manager de l'agent	Oui	Oui	Oui
Mode itinérance	Oui	Oui (Server) Non (Server Core)	Oui
Smart Feedback	Oui	Oui	Oui

Tableau 5-3. Fonctions de l'agent OfficeScan sur les plates-formes de poste de travail

Fonction	Système d'exploitation Windows			
	XP	Vista	Windows 7	Windows 8/8.1
Scan manuel, scan en temps réel et scan programmé	Oui	Oui	Oui	Oui
Mise à jour des composants (mise à jour manuelle et programmée)	Oui	Oui	Oui	Oui
Agent de mise à jour	Oui	Oui	Oui	Oui
Réputation de sites Web	Oui	Oui	Oui	Oui mais prise en charge limitée en mode Windows UI
Damage Cleanup Services	Oui	Oui	Oui	Oui
Pare-feu OfficeScan	Oui	Oui	Oui	Oui mais le filtrage d'applications n'est pas pris en charge
Surveillance des comportements	Oui (32 bits)	Oui (32 bits)	Oui (32 bits)	Oui (32 bits)
	Non (64 bits)	Oui (64 bits) La prise en charge de Vista 64-bits requiert SP1 ou SP2	Oui (64 bits)	Oui (64 bits)

Fonction	Système d'exploitation Windows			
	XP	Vista	Windows 7	Windows 8/8.1
Autoprotection de l'agent pour : • Clés de registre • Processus	Oui (32 bits)	Oui (32 bits)	Oui (32 bits)	Oui (32 bits)
	Non (64 bits)	Oui (64 bits) La prise en charge de Vista 64-bits requiert SP1 ou SP2	Oui (64 bits)	Oui (64 bits)
Autoprotection de l'agent pour : • Services • Protection des fichiers	Oui	Oui	Oui	Oui
Contrôle des dispositifs (Service de prévention des modifications non autorisées)	Oui (32 bits)	Oui (32 bits)	Oui (32 bits)	Oui (32 bits)
	Non (64 bits)	Oui (64 bits) La prise en charge de Vista 64-bits requiert SP1 ou SP2	Oui (64 bits)	Oui (64 bits)
Protection des données (y compris la fonction de protection des données du contrôle des dispositifs)	Oui (32 bits)	Oui (32 bits)	Oui (32 bits)	Oui (32 bits) en mode Poste de travail
	Oui (64 bits)	Oui (64 bits)	Oui (64 bits)	Oui (64 bits) en mode Poste de travail
Scan de la messagerie POP3	Oui	Oui	Oui	Oui

Fonction	Système d'exploitation Windows			
	XP	Vista	Windows 7	Windows 8/8.1
Plug-in Manager de l'agent	Oui	Oui	Oui	Oui
Mode itinérance	Oui	Oui	Oui	Oui
Smart Feedback	Oui	Oui	Oui	Oui

Installation de l'agent OfficeScan et prise en charge d'IPv6

Cette rubrique aborde les éléments à prendre en compte lors de l'installation de l'agent OfficeScan sur des endpoints IPv6 purs ou à double pile.

Système d'exploitation

L'agent OfficeScan ne peut être installé que sur les systèmes d'exploitation prenant en charge l'adressage IPv6 :

- Windows Vista™ (toutes les éditions)
- Windows Server 2008 (toutes les éditions)
- Windows 7 (toutes les éditions)
- Windows Server 2012 (toutes les éditions)
- Windows 8/8.1 (toutes les éditions)

Visitez le site Web suivant pour obtenir la liste complète des configurations requises :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Méthodes d'installation

Toutes les méthodes d'installation de l'agent OfficeScan peuvent être utilisées pour installer l'agent OfficeScan sur des agents IPv6 purs ou à double pile. Pour certaines

méthodes d'installation, il existe des spécifications particulières à respecter pour garantir l'installation correcte de l'agent OfficeScan.

Il n'est pas possible de faire migrer ServerProtect™ vers l'agent OfficeScan à l'aide de l'outil ServerProtect Normal Server Migration car ce dernier ne prend pas en charge l'adressage IPv6.

TABLEAU 5-4. Méthodes d'installation et prise en charge d'IPv6

MÉTHODE D'INSTALLATION	SPÉCIFICATIONS/ÉLÉMENTS À PRENDRE EN COMPTE
Page d'installation en ligne et installation sur navigateur Web	L'URL vers la page de destination comprend le nom d'hôte du serveur OfficeScan ou son adresse IP. Si vous effectuez une installation sur un agent IPv6 pur, le serveur doit être un serveur IPv6 pur ou à double pile, et son nom d'hôte ou son adresse IPv6 doit faire partie de l'URL. Quant aux agents à double pile, l'adresse IPv6 qui s'affiche dans l'écran d'état de l'installation dépend de l'option sélectionnée dans la section **Adresse IP de votre choix** sous **Agents** > **Paramètres généraux de l'agent**.
Agent Packager	Lors de l'exécution de l'outil Agent Packager, vous devrez choisir d'attribuer des privilèges d'agent de mise à jour à l'agent. N'oubliez pas qu'un agent de mise à jour IPv6 pur ne peut distribuer des mises à jour qu'à des agents IPv6 purs ou à double pile.
Conformité de sécurité, Vulnerability Scanner, et installation à distance	Un serveur IPv6 pur ne peut pas installer l'agent OfficeScan sur des endpoints IPv4 purs. De même, un serveur IPv4 pur ne peut pas installer l'agent OfficeScan sur des endpoints IPv6 purs.

Adresses IP des agents

Les serveurs OfficeScan installés dans un environnement prenant en charge l'adressage IPv6 peuvent gérer les agents OfficeScan suivants :

- Les serveurs OfficeScan installés sur des ordinateurs hôtes IPv6 purs peuvent gérer des agents IPv6 purs.

- Les serveurs OfficeScan installés sur des ordinateurs hôtes à double pile et auxquels sont affectées des adresses IPv4 et IPv6 peuvent gérer des agents IPv6 purs, des agents IPv4 purs et des agents à double pile.

Après l'installation ou la mise à niveau d'agents, ceux-ci s'enregistrent auprès du serveur à l'aide d'une adresse IP.

- Les agents IPv6 purs s'enregistrent à l'aide de leur adresse IPv6.
- Les agents IPv4 purs s'enregistrent à l'aide de leur adresse IPv4.
- Les agents à double pile s'enregistrent à l'aide de leur adresse IPv4 ou IPv6. Vous pouvez choisir l'adresse IP utilisée par ces agents.

Configuration de l'adresse IP utilisée par les agents à double pile lors de leur enregistrement auprès du serveur

Ce paramètre n'est disponible que sur les serveurs OfficeScan à double pile et ne s'applique qu'aux agents à double pile.

Procédure

1. Accédez à **Agents** > **Paramètres généraux de l'agent**.
2. Accédez à la section **Adresse IP de votre choix**.
3. Sélectionnez l'une des options suivantes :
    - **IPv4 uniquement** : les agents utilisent leur adresse IPv4.
    - **IPv4 d'abord, puis IPv6** : les agents utilisent d'abord leur adresse IPv4. Si l'agent ne peut pas s'enregistrer à l'aide de son adresse IPv4, il utilise alors son adresse IPv6. En cas d'échec de l'enregistrement avec les deux adresses IP, l'agent essaye à nouveau en suivant l'ordre de priorité établi.
    - **IPv6 d'abord, puis IPv4** : les agents utilisent d'abord leur adresse IPv6. Si l'agent ne peut pas s'enregistrer à l'aide de son adresse IPv6, il utilise alors son adresse IPv4. En cas d'échec de l'enregistrement avec les deux adresses IP, l'agent essaye à nouveau en suivant l'ordre de priorité établi.

4. Cliquez sur **Enregistrer**.

Éléments à prendre en compte pour le déploiement

Cette section récapitule les différentes méthodes permettant d'effectuer une nouvelle installation de l'agent OfficeScan. Toutes les méthodes d'installation requièrent des droits d'administration locaux sur les ordinateurs cibles.

Si vous installez des agents et que vous souhaitez activer la prise en charge d'IPv6, consultez les instructions de la rubrique *Installation de l'agent OfficeScan et prise en charge d'IPv6 à la page 5-8*.

TABLEAU 5-5. Considérations de déploiement de l'installation

MÉTHODE D'INSTALLATION/PRISE EN CHARGE DU SYSTÈME D'EXPLOITATION	ÉLÉMENTS À PRENDRE EN COMPTE POUR LE DÉPLOIEMENT					
	DÉPLOIEMENT SUR UN WAN	GESTION CENTRALISÉE	REQUIERT L'INTERVENTION DE L'UTILISATEUR	NÉCESSITE UNE RESSOURCE INFORMATIQUE	DÉPLOIEMENT DE MASSE	BANDE PASSANTE CONSOMMÉE
Page Web d'installation Prise en charge sur tous les systèmes d'exploitation sauf Windows Server Core 2008 et Windows 8/8.1/ Server 2012/Server Core 2012 en mode Windows UI	Non	Non	Oui	Non	Non	Élevé

Méthode d'installation/Prise en charge du système d'exploitation	Éléments à prendre en compte pour le déploiement					
	Déploiement sur un WAN	Gestion centralisée	Requiert l'intervention de l'utilisateur	Nécessite une ressource informatique	Déploiement de masse	Bande passante consommée
Installations basées sur navigateur Prise en charge sur tous les systèmes d'exploitation **Remarque** Non prise en charge sur Windows 8, 8.1 ni Windows Server 2012 en mode Windows UI.	Non	Non	Oui	Oui	Non	Élevée si les installations sont lancées simultanément
Installations en mode UNC Prise en charge sur tous les systèmes d'exploitation	Non	Non	Oui	Oui	Non	Élevée si les installations sont lancées simultanément

Méthode d'installation/Prise en charge du système d'exploitation	Éléments à prendre en compte pour le déploiement					
	Déploiement sur un WAN	Gestion centralisée	Requiert l'intervention de l'utilisateur	Nécessite une ressource informatique	Déploiement de masse	Bande passante consommée
Installations à distance Prise en charge sur tous les systèmes d'exploitation sauf : • Windows Vista Édition Familiale Basique et Édition Familiale Premium • Windows XP Édition Familiale • Windows 7 Édition Familiale Basique/Édition Familiale Premium • Windows 8/8.1 (versions basiques)	Non	Oui	Non	Oui	Non	Élevé

Méthode d'installation/Prise en charge du système d'exploitation	Éléments à prendre en compte pour le déploiement					
	Déploiement sur un WAN	Gestion centralisée	Requiert l'intervention de l'utilisateur	Nécessite une ressource informatique	Déploiement de masse	Bande passante consommée
Configuration du script de connexion Prise en charge sur tous les systèmes d'exploitation	Non	Non	Oui	Oui	Non	Élevée si les installations sont lancées simultanément
Agent Packager Prise en charge sur tous les systèmes d'exploitation	Non	Non	Oui	Oui	Non	Faible si programmée
Agent Packager (package MSI déployé via Microsoft SMS) Prise en charge sur tous les systèmes d'exploitation	Oui	Oui	Oui/Non	Oui	Oui	Faible si programmée
Agent Packager (package MSI déployé via Active Directory) Prise en charge sur tous les systèmes d'exploitation	Oui	Oui	Oui/Non	Oui	Oui	Élevée si les installations sont lancées simultanément

Méthode d'installation/Prise en charge du système d'exploitation	Éléments à prendre en compte pour le déploiement					
	Déploiement sur un WAN	Gestion centralisée	Requiert l'intervention de l'utilisateur	Nécessite une ressource informatique	Déploiement de masse	Bande passante consommée
Image disque de l'agent Prise en charge sur tous les systèmes d'exploitation	Non	Non	Non	Oui	Non	Faible
Trend Micro Vulnerability Scanner (TMVS) Prise en charge sur tous les systèmes d'exploitation sauf : • Windows Vista Édition Familiale Basique et Édition Familiale Premium • Windows XP Édition Familiale • Windows 8/8.1 (versions basiques)	Non	Oui	Non	Oui	Non	Élevé

Méthode d'installation/Prise en charge du système d'exploitation	Éléments à prendre en compte pour le déploiement					
	Déploiement sur un WAN	Gestion centralisée	Requiert l'intervention de l'utilisateur	Nécessite une ressource informatique	Déploiement de masse	Bande passante consommée
Installations de la conformité de sécurité Prise en charge sur tous les systèmes d'exploitation sauf : • Windows Vista Édition Familiale Basique et Édition Familiale Premium • Windows XP Édition Familiale • Windows 7 Édition Familiale Basique/Édition Familiale Premium • Windows 8/8.1 (versions basiques)	Non	Oui	Non	Oui	Non	Élevé

Installations de la page Web d'installation

Les utilisateurs peuvent installer le programme de l'agent OfficeScan à partir de la page Web d'installation si vous le serveur OfficeScan se trouve sur un endpoint fonctionnant sous les plates-formes suivantes :

- Windows Server 2003 avec Internet Information Server (IIS) 6.0 ou Apache 2.0.x
- Windows Server 2008 avec Internet Information Server (IIS) 7.0
- Windows Server 2008 R2 avec Internet Information Server (IIS) 7.5
- Windows Server 2012 avec Internet Information Server (IIS) 8.0

Pour procéder à l'installation depuis la page Web d'installation, vous devez disposer des éléments suivants :

- Internet Explorer avec le niveau de sécurité défini de manière à autoriser les contrôles ActiveX™. Les versions requises sont les suivantes :
  - 6.0 sous Windows XP et Windows Server 2003
  - 7.0 sous Windows Vista et Windows Server 2008
  - 8.0 sous Windows 7
  - 10.0 sous Windows 8/8.1 et Windows Server 2012
- Privilèges d'administrateur sur le endpoint

Pour que les utilisateurs installent l'agent OfficeScan depuis la page Web d'installation, envoyez-leur les instructions suivantes. Pour envoyer une notification d'installation par courrier électronique, voir *Installation basée sur un navigateur à la page 5-19*.

Installation depuis la page Web d'installation

Procédure

1. Connectez-vous au endpoint à l'aide d'un compte administrateur intégré.



Remarque

Pour les plates-formes Windows 7, 8 ou 8.1, vous devez au préalable activer le compte d'administrateur intégré. Par défaut, Windows 7, 8 et 8.1 désactivent ce compte. Pour plus d'informations, consultez le site de l'assistance technique de Microsoft (http://technet.microsoft.com/en-us/library/dd744293%28WS.10%29.aspx).

2. En cas d'installation sur un endpoint fonctionnant sous Windows XP, Vista, 7, 8, 8.1, Server 2008 ou Server 2012, effectuez les opérations suivantes :

   a. Lancez Internet Explorer et ajoutez l'URL du serveur OfficeScan (telle que `https://<nom du serveur OfficeScan>:4343/officescan`) à la liste des sites sécurisés. Dans Windows XP Édition Familiale, il est possible d'accéder à la liste en se rendant sous **Outils** > **Options internet** > **onglet Sécurité**, en sélectionnant l'icône **Sites de confiance** et en cliquant sur **Sites**.

   b. Modifiez le paramètre de sécurité d'Internet Explorer en activant l'option **Demander confirmation pour les contrôles Active X**. Sous Windows XP, accédez à **Outils** > **Options internet** > **onglet Sécurité**, et cliquez sur **Personnaliser le niveau**.

3. Ouvrez une fenêtre Internet Explorer et saisissez ce qui suit :

   ```
   https://<nom du serveur OfficeScan>:<port>/officescan
   ```

4. Cliquez sur le lien **programme d'installation** de la page de connexion pour afficher les options d'installation suivantes :

   - **Installation d'agent basée sur navigateur** (Internet Explorer uniquement) : suivez les instructions qui s'affichent à l'écran selon votre système d'exploitation.

   - **Installation de l'agent MSI** : téléchargez le package 32 bits ou 64 bits, en fonction de votre système d'exploitation, et suivez les instructions qui s'affichent à l'écran.



Remarque

Autorisez l'installation du contrôle ActiveX si vous y êtes invité.

5. Une fois l'installation terminée, l'icône de l'agent OfficeScan apparaît dans la barre d'état système de Windows.



Remarque

Pour une liste des icônes qui s'affichent dans la barre d'état système, reportez-vous à *Icônes de l'agent OfficeScan à la page 14-27*.

Installation basée sur le navigateur

Dans cet écran, vous pouvez définir un message électronique demandant aux utilisateurs du réseau d'installer l'agent OfficeScan. Pour démarrer l'installation, les utilisateurs doivent cliquer sur le lien vers le programme d'installation de l'agent OfficeScan, fourni dans le message électronique.

Avant d'installer des agents OfficeScan :

- Vérifiez la configuration minimale requise pour l'installation de l'agent OfficeScan.
- Identifiez les ordinateurs de votre réseau ne disposant pas d'une protection contre les risques de sécurité. Effectuez les actions suivantes :
  - Exécutez Trend Micro Vulnerability Scanner. Cet outil recherche les programmes antivirus installés sur les endpoints en fonction d'une plage d'adresses IP que vous spécifiez. Pour obtenir des informations détaillées, voir *Utilisation de Vulnerability Scanner à la page 5-40*.
  - Exécutez des tests de conformité de sécurité. Pour obtenir des informations détaillées, voir *Conformité de la sécurité pour les endpoints non gérés à la page 14-71*.

Installation basée sur un navigateur

Procédure

1. Accédez à **Agents** > **Installation de l'agent** > **Basé sur navigateur**.
2. Si nécessaire, modifiez l'objet du message électronique.
3. Cliquez sur **Créer un courrier électronique.**.

Votre programme de messagerie par défaut s'ouvre automatiquement.

4. Envoyez le message électronique aux destinataires choisis.

Exécution d'une installation basée sur UNC

AutoPcc.exe est un programme autonome qui installe l'agent OfficeScan sur les ordinateurs non protégés et met à jour les fichiers du programme et les composants. Les endpoints doivent faire partie du domaine pour pouvoir utiliser AutoPcc via un chemin UNC (Uniform Naming Convention).

Procédure

1. Accédez à **Agents** > **Installation de l'agent** > **En mode UNC**.

    - Pour installer l'agent OfficeScan sur un endpoint non protégé à l'aide de AutoPcc.exe :

        a. Connectez-vous au serveur. Accédez au chemin UNC :

        ```
        \\<nom de l'ordinateur du serveur>\ofscan
        ```

        b. Cliquez avec le bouton droit de la souris sur AutoPcc.exe et sélectionnez **Exécuter en tant qu'administrateur**.

    - Pour une installation sur un poste de travail distant à l'aide d'AutoPcc.exe :

        a. Ouvrez une connexion Remote Desktop Connection (Mstsc.exe) en mode console. Cela force l'installation par AutoPcc.exe à s'effectuer lors de la session 0.

        b. Accédez au répertoire \\<nom de l'ordinateur du serveur>\ofscan et exécutez AutoPcc.exe.

Installation à distance depuis OfficeScan Web Console

Vous pouvez installer l'agent OfficeScan à distance sur un ou plusieurs ordinateurs connectés au réseau. Vérifiez si vous disposez de droits d'administrateur sur les

ordinateurs cibles pour effectuer l'installation à distance. L'outil d'installation à distance n'installe pas l'agent OfficeScan sur les endpoints exécutant le serveur OfficeScan.



Remarque

Cette méthode d'installation ne peut pas être employée sur les endpoints fonctionnant sous Windows XP Édition Familiale, Windows Vista Édition Familiale Basique ou Édition Familiale Premium, Windows 7 Édition Familiale Basique ou Édition Familiale Premium (versions 32 bits et 64 bits) ni Windows 8/8.1 (versions basiques 32 bits et 64 bits). Un serveur IPv6 pur ne peut pas installer l'agent OfficeScan sur des agents IPv4 purs. De même, un serveur IPv4 pur ne peut pas installer l'agent OfficeScan sur des agents IPv6 purs.

Procédure

1. En cas d'exécution sous Windows Vista, Windows 7, Windows 8 (Édition professionnelle, Édition Entreprise), Windows 8.1 ou Windows Server 2012, effectuez les étapes suivantes :

   a. Activez un compte administrateur intégré et définissez un mot de passe pour le compte.

   b. Désactivez le partage de fichier simple sur le endpoint.

   c. Cliquez sur **Démarrer** > **Tous les programmes** > **Outils administrateurs** > **Pare-feu Windows avec fonctions avancées de sécurité**.

   d. Pour Profil de domaine, Profil privé et Profil public, configurez l'état du pare-feu sur « Désactivé ».

   e. Ouvrez Microsoft Management Console (cliquez sur **Démarrer** > **Exécuter** et entrez `services.msc`) puis démarrez les services **Accès à distance**et **Appel de procédure à distance**. Lors de l'installation de l'agent OfficeScan, utilisez le compte administrateur intégré et le mot de passe correspondant.

2. Sur la console Web, accédez à **Agents** > **Installation de l'agent** > **Distant**.

3. Sélectionnez les ordinateurs cibles.

   - La liste **Domaines et endpoints** répertorie tous les domaines Windows du réseau. Pour afficher les endpoints d'un domaine, double-cliquez sur le nom du domaine. Sélectionnez un endpoint et cliquez sur **Ajouter**.

- Si vous souhaitez utiliser un nom de endpoint spécifique, saisissez-le dans le champ **Recherche de endpoints** en haut de la page et appuyez sur la touche Entrée.

OfficeScan vous invite à fournir le nom d'utilisateur et le mot de passe de l'ordinateur cible. Pour pouvoir continuer, assurez-vous que votre nom d'utilisateur et votre mot de passe correspondent à un compte administrateur.

4. Saisissez le nom d'utilisateur et le mot de passe, puis cliquez sur **Connexion**.

   Le endpoint cible s'affiche dans le tableau **Endpoints sélectionnés**.

5. Répétez les étapes 3 et 4 pour ajouter d'autres ordinateurs.

6. Cliquez sur **Installer** lorsque vous êtes prêt à installer l'agent OfficeScan sur les ordinateurs cibles.

   Une fenêtre de confirmation apparaît.

7. Cliquez sur **Oui** pour confirmer l'installation de l'agent OfficeScan sur les ordinateurs cibles.

   Un écran s'affiche, indiquant la progression de la copie des fichiers du programme sur chaque endpoint cible.

Lorsqu'OfficeScan a terminé l'installation sur un endpoint cible, le nom de ce endpoint disparaît de la liste **Endpoints sélectionnés** et s'affiche dans la liste **Domaines et endpoints** avec une coche rouge.

L'installation à distance est terminée lorsque tous les ordinateurs cibles apparaissent accompagnés d'une coche rouge dans la liste **Domaines et endpoints**.



Remarque

Si vous exécutez l'installation sur plusieurs ordinateurs, OfficeScan enregistre tout échec dans les journaux (pour plus d'informations, voir *Journaux des nouvelles installations à la page 16-17*) tout en procédant aux autres installations. Il n'est pas nécessaire de superviser l'installation après avoir cliqué sur **Installer**. Vérifiez les journaux ultérieurement pour voir les résultats de l'installation.

Installation avec l'outil Configuration du script de connexion

L'outil Configuration du script de connexion permet d'automatiser l'installation de l'agent OfficeScan sur des ordinateurs non protégés lorsqu'ils se connectent au réseau. Il ajoute un programme appelé `AutoPcc.exe` dans le script de connexion au serveur.

`AutoPcc.exe` installe l'agent OfficeScan sur les endpoints non protégés et met à jour les fichiers du programme et les composants. Les endpoints doivent faire partie du domaine pour pouvoir utiliser AutoPcc à l'aide du script de connexion.

Installation de l'agent OfficeScan

`AutoPcc.exe` installe automatiquement l'agent OfficeScan sur un endpoint Windows Server 2003 non protégé lors de la connexion de ce dernier au serveur dont vous avez modifié les scripts de connexion. Cependant, `AutoPcc.exe` n'installe pas automatiquement l'agent OfficeScan sur les ordinateurs Windows Vista, 7, 8, 8.1, Server 2008 ni Server 2012. Les utilisateurs doivent se connecter à l'ordinateur du serveur, accéder au répertoire `\\<nom de l'ordinateur du serveur>\ofcscan`, effectuer un clic droit sur `AutoPcc.exe` et sélectionner **Exécuter en tant qu'administrateur**.

Pour une installation sur un poste de travail distant à l'aide d'`AutoPcc.exe` :

- Le endpoint doit s'exécuter en mode `Mstsc.exe /console`. Cela force l'installation par `AutoPcc.exe` à s'effectuer lors de la session 0.
- Mappez un lecteur sur le dossier partagé « ofcscan » et exécutez `AutoPcc.exe` depuis cet emplacement.

Mises à jour de programmes et de composants

`AutoPcc.exe` met à jour les fichiers programme ainsi que les composants antivirus, anti-spywares et Damage Cleanup Services.

Scripts pour Windows Server 2003, 2008 et 2012

Si vous disposez déjà d'un script de connexion, l'outil Configuration du script de connexion ajoute une commande permettant d'exécuter `AutoPcc.exe`. Sinon,

OfficeScan crée un fichier batch appelé `ofcscan.bat` qui contient la commande d'exécution du programme `AutoPcc.exe`.

L'outil Configuration du script de connexion ajoute la ligne suivante à la fin du script :

```
\\<Server_name>\ofcscan\autopcc
```

Où :

- `<Nom_du_serveur>` correspond au nom ou à l'adresse IP du endpoint sur lequel est installé le serveur OfficeScan.
- "« `ofcscan` » correspond au dossier partagé OfficeScan sur le serveur.
- "« `autopcc` » est le lien vers le fichier exécutable autopcc qui installe l'agent OfficeScan.

Emplacement du script de connexion (via un répertoire partagé Netlogon) :

- `Windows Server 2003 : \\Windows 2003 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`
- `Windows Server 2008 : \\Windows 2008 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`
- `Windows Server 2012 : \\Windows 2012 server\system drive \windir\sysvol\domain\scripts\ofcscan.bat`

Ajout d'Autopcc.exe au script de connexion à l'aide de l'outil Configuration du script de connexion

Procédure

1. Sur le endpoint que vous avez utilisé pour exécuter l'installation du serveur, dans le menu Démarrer de Windows, cliquez sur **Programmes** > **Trend Micro OfficeScan Server <Nom du serveur>** > **Configuration du script de connexion**.

   L'outil **Configuration du script de connexion** se charge. La console affiche une arborescence présentant tous les domaines du réseau.

2. Recherchez le serveur dont vous souhaitez modifier le script de connexion, sélectionnez-le, puis cliquez sur **Sélectionner**. Vérifiez que ce serveur est un contrôleur de domaine principal et que vous disposez d'un accès d'administrateur à celui-ci.

   L'outil Configuration du script de connexion vous demande alors un nom d'utilisateur et un mot de passe.

3. Saisissez le nom d'utilisateur et le mot de passe. Cliquez sur **OK** pour continuer.

   La fenêtre **Sélection des utilisateurs** apparaît. La liste **Utilisateurs** affiche les profils des utilisateurs qui se connectent au serveur, tandis que la liste **Utilisateurs sélectionnés** affiche uniquement les profils des utilisateurs dont vous souhaitez modifier le script de connexion.

4. Pour modifier le script de connexion d'un profil utilisateur, faites votre sélection dans la liste **Utilisateurs**, puis cliquez sur **Ajouter**.

5. Pour modifier le script de connexion de tous les utilisateurs, cliquez sur **Ajouter tout**.

6. Pour retirer un profil utilisateur précédemment sélectionné, choisissez son nom dans la liste **Utilisateurs sélectionnés**, puis cliquez sur **Supprimer**.

7. Pour réinitialiser vos choix, cliquez sur **Supprimer tout**.

8. Cliquez sur **Appliquer** lorsque tous les profils d'utilisateurs cibles sont affichés dans la liste **Utilisateurs sélectionnés**.

   Un message vous informe que vous avez modifié avec succès les différents scripts de connexion.

9. Cliquez sur **OK**.

   L'outil Configuration du script de connexion retrouve alors son aspect initial.

10. Pour modifier les scripts de connexion d'autres serveurs, répétez simplement les étapes 2 à 4.

11. Pour fermer l'outil Configuration du script de connexion, cliquez sur **Quitter**.

Installation à l'aide de l'outil Agent Packager

L'outil Agent Packager créé un package d'installation que vous pouvez envoyer aux utilisateurs via des supports traditionnels tels qu'un CD-ROM. Les utilisateurs exécutent le package sur le endpoint de l'agent pour installer ou mettre à niveau l'agent OfficeScan et mettre à jour les composants.

L'outil Agent Packager est particulièrement utile pour déployer l'agent OfficeScan ou des composants sur des agents situés dans des bureaux distants disposant d'une faible bande passante. Les agents OfficeScan installés à l'aide de l'outil Agent Packager communiquent avec le serveur sur lequel a été créé le package d'installation.

L'outil Agent Packager requiert les éléments suivants :

- 350 Mo d'espace disque disponible
- Windows Installer 2.0 (pour pouvoir exécuter un pack MSI).

Instructions pour le déploiement du pack

1. Envoyez le package aux utilisateurs et demandez-leur d'exécuter le package de l'agent OfficeScan sur leur ordinateur en double-cliquant sur le fichier `.exe` ou `.msi`.



Remarque

Envoyez le package uniquement aux utilisateurs dont l'agent OfficeScan dépendra du serveur sur lequel le package a été créé.

2. Si certains utilisateurs comptent installer le package `.exe` sur des ordinateurs fonctionnant sous Windows Vista, 7, 8, 8.1, Server 2008 ou Server 2012, invitez-les à effectuer un clic droit sur le fichier `.exe`, puis à sélectionner **Exécuter en tant qu'administrateur**.
3. Si vous avez créé un fichier `.msi`, déployez le pack en effectuant les tâches suivantes :
    - Utiliser Active Directory ou Microsoft SMS. Voir *Déploiement d'un package MSI à l'aide d'Active Directory à la page 5-32* ou *Déploiement d'un pack MSI à l'aide de Microsoft SMS à la page 5-34*.

4. Lancez le package MSI depuis une fenêtre d'invite de commandes pour installer l'agent OfficeScan en mode silencieux sur un endpoint distant fonctionnant sous Windows XP, Vista, 7, 8, 8.1, Server 2008 ou Server 2012.

Instructions relatives aux méthodes de scan pour les packages d'agents

Sélectionnez la méthode de scan du pack. Voir *Types de méthodes de scan à la page 7-9* pour obtenir des informations détaillées.

Les composants inclus dans le pack dépendent de la méthode de scan que vous avez sélectionnée. Pour plus d'informations sur les composants disponibles pour chaque méthode de scan, voir *Mises à jour des agents OfficeScan à la page 6-31*.

Avant de sélectionner la méthode de scan, prenez en compte les directives suivantes pour déployer efficacement le pack :

- Si le package est destiné à mettre à niveau un agent vers cette version d'OfficeScan, vérifiez la méthode de scan au niveau du domaine sur la console Web. Sur la console, accédez à **Agents** > **Gestion des agents**, sélectionnez le domaine de l'arborescence des agents auquel appartient l'agent, puis cliquez sur **Paramètres** > **Paramètres de scan** > **Méthodes de scan**. La méthode de scan du niveau domaine doit être cohérente avec celle du pack.

- Si vous prévoyez d'utiliser le package pour effectuer une nouvelle installation de l'agent OfficeScan, vérifiez le paramètre du regroupement des agents. Sur la console Web, accédez à **Agents** > **Regroupement des agents**.

- Si les agents sont regroupés par domaine NetBIOS, Active Directory ou DNS, vérifiez à quel domaine appartient le endpoint cible. Si le domaine existe, vérifiez la méthode de scan configurée pour le domaine. Si le domaine n'existe pas, vérifiez la méthode de scan du niveau racine (sélectionnez l'icône du domaine racine () dans l'arborescence des agents et cliquez sur **Paramètres** > **Paramètres de scan** > **Méthodes de scan**). La méthode de scan du domaine ou du niveau racine doit être cohérente avec celle du pack.

- Si les agents sont regroupés par groupes d'agents personnalisés, vérifiez les options **Priorité de regroupement** et **Source**.

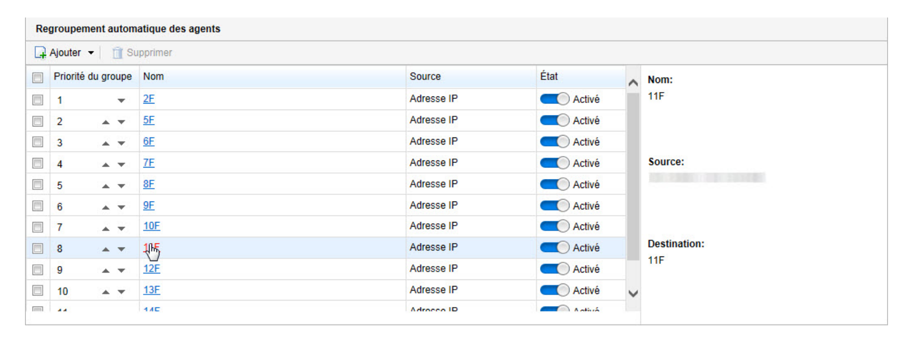


FIGURE 5-1. Volet d'aperçu du regroupement automatique des agents

Si le endpoint cible appartient à une source spécifique, vérifiez l'option **Destination** correspondante. La destination est indiquée par le nom de domaine qui s'affiche dans l'arborescence des agents. Une fois l'installation terminée, l'agent appliquera la méthode de scan propre à ce domaine.

- Si le package est destiné à mettre à jour les composants de l'agent à l'aide de cette version d'OfficeScan, vérifiez la méthode de scan configurée pour le domaine de l'arborescence des agents auquel l'agent appartient. La méthode de scan du niveau domaine doit être cohérente avec celle du pack.

Considérations relatives à l'agent de mise à jour

Affectez à l'agent OfficeScan des privilèges d'agent de mise à jour sur le endpoint cible. Les agents de mise à jour aident le serveur OfficeScan à déployer des composants sur les agents. Pour obtenir des informations détaillées, voir *Agents de mise à jour à la page 6-60*.

Si vous attribuez des privilèges d'agent de mise à jour à un agent OfficeScan :

1. N'oubliez pas que si le package est déployé sur un endpoint IPv6 pur, l'agent de mise à jour ne peut distribuer des mises à jour qu'à des agents IPv6 purs ou à double pile.

2. Utilisez l'outil de configuration des mises à jour programmées pour activer et configurer les mises à jour programmées pour l'agent. Pour obtenir des

informations détaillées, voir *Méthodes de mise à jour pour les agents de mise à jour à la page 6-67*.

3. Le serveur OfficeScan qui gère l'agent de mise à jour ne pourra pas synchroniser ou déployer les paramètres suivants sur l'agent :

   - Privilège d'agent de mise à jour
   - Mise à jour programmée de l'agent
   - Mises à jour depuis le serveur ActiveUpdate de Trend Micro
   - Mises à jour depuis d'autres sources de mise à jour

   Par conséquent, déployez le package de l'agent OfficeScan uniquement sur les ordinateurs qui ne seront pas gérés par un serveur OfficeScan. Par la suite, configurez l'agent de mise à jour pour qu'il obtienne ses mises à jour d'une source autre que le serveur OfficeScan, par exemple une source de mise à jour personnalisée. Si vous souhaitez que le serveur OfficeScan synchronise ses paramètres avec l'agent de mise à jour, n'utilisez pas l'outil Agent Packager et choisissez une autre méthode d'installation de l'agent OfficeScan.

Création d'un package d'installation à l'aide de l'outil Agent Packager

Procédure

1. Sur l'ordinateur du serveur OfficeScan, accédez au répertoire <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\ClientPackager`.

2. Cliquez deux fois sur le fichier `ClnPack.exe` pour exécuter l'outil.

La console de l'outil **Agent Packager** s'ouvre.

3. Sélectionnez le type de pack que vous désirez créer.

TABLEAU 5-6. Types de packages d'agents

TYPE DE PACK	DESCRIPTION
Installation	Sélectionnez **Installation** pour créer le pack sous forme de fichier exécutable. Le package installe le programme de l'agent OfficeScan avec les composants actuellement disponibles sur le serveur. Si une version précédente de l'agent OfficeScan est installée sur le endpoint cible, le lancement du fichier exécutable met l'agent à niveau.
Mise à jour	Sélectionnez **Mise à jour** pour créer un pack contenant les composants actuellement disponibles sur le serveur. Le pack sera créé sous forme de fichier exécutable. Utilisez ce package si vous rencontrez des problèmes lors de la mise à jour de composants sur le endpoint d'un agent.
MSI	Sélectionnez **MSI** pour créer un pack conforme au format de pack de Microsoft Installer. Le package installe également le programme de l'agent OfficeScan avec les composants actuellement disponibles sur le serveur. Si une version précédente de l'agent OfficeScan est installée sur le endpoint cible, le lancement du fichier MSI met l'agent à niveau.

4. Sélectionnez le système d'exploitation pour lequel vous voulez créer le package. Veillez à ne déployer le package que sur des endpoints exécutant ce type de système d'exploitation. Créez un autre package pour effectuer un déploiement sur un autre type de système d'exploitation.

5. Sélectionnez la méthode de scan déployée par le package de l'agent.

   Pour obtenir des instructions sur la sélection d'une méthode de scan, voir *Instructions relatives aux méthodes de scan pour les packages d'agents à la page 5-27*.

6. Dans la section **Domaine**, sélectionnez l'une des options suivantes :

   - **Autoriser l'agent à indiquer automatiquement son domaine** : après l'installation de l'agent OfficeScan, celui-ci interroge la base de données du serveur OfficeScan et indique ses paramètres de domaine au serveur.

   - N'importe quel domaine de la liste : l'outil Agent Packager se synchronise avec le serveur OfficeScan et répertorie les domaines actuellement utilisés dans l'arborescence des agents.

7. Dans la section **Options**, sélectionnez l'une des options suivantes :

OPTION	DESCRIPTION
Mode silencieux	Cette option crée un package qui s'installe en arrière-plan sur le endpoint de l'agent, de façon entièrement transparente et sans l'affichage d'aucune fenêtre d'état de l'installation. Activez cette option si vous prévoyez de déployer le package à distance sur le endpoint cible.
Forcer l'écrasement par la dernière version	Cette option remplace les versions des composants sur l'agent par les versions actuellement disponibles sur le serveur. Activez cette option pour assurer la synchronisation des composants du serveur et de l'agent.
Désactiver le pré-scan (nouvelles installations uniquement)	Si l'agent OfficeScan n'est pas installé sur le endpoint cible, le package scanne préalablement le endpoint à la recherche de risques de sécurité avant d'installer l'agent OfficeScan. Si vous êtes certain que le endpoint cible n'est pas infecté par des risques de sécurité, désactivez le pré-scan. Si le pré-scan est activé, le programme d'installation scanne les zones les plus vulnérables du endpoint, notamment les zones suivantes, à la recherche de virus et de programmes malveillants : • La zone et le répertoire d'amorçage (contre les virus d'amorce). • Le dossier Windows. • Le dossier Program Files.

8. Sous **Fonctions de l'Agent de mise à jour**, sélectionnez les fonctionnalités pouvant être déployées par l'agent de mise à jour.

   Pour en savoir plus sur l'affectation de fonctions de l'agent de mise à jour, voir *Considérations relatives à l'agent de mise à jour à la page 5-28*.

9. Sous **Composants**, sélectionnez les composants et fonctionnalités à inclure dans le package.

   - Pour plus de détails sur les composants, voir *Composants et programmes OfficeScan à la page 6-2*.

- Le module Protection des données n'est disponible que si vous installez et activez la protection des données. Pour plus d'informations sur la protection des données, voir *Démarrage de la protection des données à la page 3-1*.

10. À côté de **Fichier source**, assurez-vous que l'emplacement du fichier `ofcscan.ini` est correct. Pour modifier le chemin d'accès, cliquez sur [...] pour accéder au fichier `ofcscan.ini`.

Par défaut, ce fichier se trouve dans le répertoire `<dossier d'installation du serveur>\PCCSRV` du serveur OfficeScan.

11. Dans **Fichier de sortie**, cliquez sur [...] et indiquez l'emplacement où vous souhaitez créer le package de l'agent OfficeScan, ainsi que le nom du fichier (par exemple `AgentSetup.exe`).

12. Cliquez sur **Créer**.

Lorsque l'outil Agent Packager a fini de créer le package, le message « Création du package réussie » s'affiche.« » Recherchez le pack dans le répertoire que vous avez spécifié dans l'étape précédente.

13. Déployez le pack.

Déploiement d'un package MSI à l'aide d'Active Directory

Profitez des fonctionnalités d'Active Directory pour déployer le package MSI sur plusieurs endpoints d'agents simultanément. Pour obtenir des instructions sur la création d'un fichier MSI, voir *Installation à l'aide de l'outil Agent Packager à la page 5-26*.

Procédure

1. Effectuez les opérations suivantes :

- Pour Windows Server 2003 et versions antérieures :

  a. Ouvrez la console Active Directory.

  b. Cliquez avec le bouton droit de la souris sur l'unité d'organisation (UO) sur laquelle vous souhaitez déployer le package MSI et cliquez sur **Propriétés**.

c. Sous l'onglet **Stratégie de groupe**, cliquez sur **Nouveau**.

- Pour Windows Server 2008 et Windows Server 2008 R2 :

   a. Ouvrez la **console de gestion des stratégies de groupe**. Cliquez sur **Démarrer** > **Panneau de configuration** > **Outils d'administration** > **Gestion des stratégies de groupe**.

   b. Dans l'arborescence de la console, développez **Objets de stratégie de groupe** dans la forêt et le domaine contenant l'objet de stratégie de groupe que vous souhaitez modifier.

   c. Cliquez avec le bouton droit de la souris sur l'objet de stratégie de groupe à modifier, puis cliquez sur **Modifier**. L'**Éditeur d'objets de stratégie de groupe** s'ouvre.

- Pour Windows Server 2012 :

   a. Ouvrez la **console de gestion des stratégies de groupe**. Cliquez sur **Gestion de serveur** > **Outils** > **Gestion des stratégies de groupe**.

   b. Dans l'arborescence de la console, développez **Objets de stratégie de groupe** dans la forêt et le domaine contenant l'objet de stratégie de groupe que vous souhaitez modifier.

   c. Cliquez avec le bouton droit de la souris sur l'objet de stratégie de groupe à modifier, puis cliquez sur **Modifier**. L'**Éditeur d'objets de stratégie de groupe** s'ouvre.

2. Choisissez entre **Configuration ordinateur** et **Configuration utilisateur** et ouvrez **Paramètres du logiciel** affiché en dessous.



Conseil

Trend Micro recommande d'utiliser **Configuration ordinateur** au lieu de **Configuration utilisateur** pour garantir le succès de l'installation du package MSI indépendamment de l'utilisateur qui se connecte au endpoint.

3. Sous **Paramètres du logiciel**, cliquez avec le bouton droit de la souris sur **Installation de logiciel**, puis sélectionnez **Nouveau** et **Package**.

4. Déterminez l'emplacement du pack MSI et sélectionnez-le.

5. Sélectionnez une méthode de déploiement et cliquez sur **OK**.

    - **Attribué** : Le package MSI est déployé automatiquement lors de la prochaine connexion d'un utilisateur sur le endpoint (si vous avez sélectionné Configuration utilisateur) ou lors du redémarrage du endpoint (si vous avez sélectionné Configuration ordinateur). Cette méthode ne nécessite pas l'intervention de l'utilisateur.

    - **Publié** : Pour lancer le pack MSI, demandez aux utilisateurs d'accéder au Panneau de configuration, ouvrez l'écran Ajout/Suppression de programmes et sélectionnez l'option permettant d'ajouter/d'installer des programmes sur le réseau. Lorsque le package MSI de l'agent OfficeScan s'affiche, les utilisateurs peuvent procéder à l'installation de l'agent OfficeScan.

Déploiement d'un pack MSI à l'aide de Microsoft SMS

Déployez le pack MSI à l'aide Microsoft SMS (System Management Server) si Microsoft BackOffice SMS est installé sur le serveur. Pour obtenir des instructions sur la création d'un fichier MSI, voir *Installation à l'aide de l'outil Agent Packager à la page 5-26*.

Le serveur SMS doit obtenir le fichier MSI du serveur OfficeScan avant de pouvoir déployer le pack vers les ordinateurs cibles.

- Local : le serveur SMS et le serveur OfficeScan se trouvent sur le même endpoint.

- Distant : Le serveur SMS et le serveur OfficeScan sont sur des ordinateurs différents.

Problèmes connus lors de l'installation avec Microsoft SMS :

- « Inconnu » s'affiche dans la colonne **Durée d'exécution** de la console SMS.

- Le moniteur de programme SMS peut indiquer que l'installation est terminée, même en cas d'échec de celle-ci. Pour obtenir des instructions sur la vérification de la réussite de l'installation, voir *Tâches après l'installation à la page 5-71*.

Les instructions suivantes sont valables si vous utilisez Microsoft SMS 2.0 et 2003.

Obtention d'un pack en local

Procédure

1. Ouvrez la console **Administrateur SMS**.
2. Sous l'onglet **Arborescence**, cliquez sur **Packages**.
3. Dans le menu **Action**, cliquez sur **Nouveau** > **Pack à partir d'une définition**.

   L'écran **Bienvenue** de l'**Assistant Création de lot à partir d'une définition** apparaît.
4. Cliquez sur **Suivant**.

   L'écran **Définition du pack** apparaît.
5. Cliquez sur **Parcourir**.

   L'écran **Ouvrir** apparaît.
6. Recherchez et sélectionnez le fichier du package MSI créé par l'outil Agent Packager, puis cliquez sur **Ouvrir**.

   Le nom du pack MSI apparaît dans l'écran **Définition du package**. Le package indique « Agent OfficeScan » et la version du programme.
7. Cliquez sur **Suivant**.

   L'écran **Fichiers sources** apparaît.
8. Cliquez sur **Toujours obtenir les fichiers du répertoire source**, puis sur **Suivant**.

   L'écran **Répertoire source** apparaît ; il affiche le nom du pack que vous souhaitez créer, ainsi que le répertoire source.
9. Cliquez sur **Lecteur local sur le serveur de site**.
10. Cliquez sur **Parcourir** et sélectionnez le répertoire source contenant le fichier MSI.
11. Cliquez sur **Suivant**.

L'assistant crée le pack. Une fois le processus terminé, le nom du pack apparaît sur la console **Administrateur SMS**.

Obtention d'un pack à distance

Procédure

1. Sur le serveur OfficeScan, utilisez l'outil Agent Packager pour créer un package d'installation portant une extension `.exe` (vous ne pouvez pas créer de package `.msi`). Voir *Installation à l'aide de l'outil Agent Packager à la page 5-26* pour obtenir des informations détaillées.

2. Créez un dossier partagé sur le endpoint sur lequel vous voulez stocker la source.

3. Ouvrez la console Administrateur SMS.

4. Sous l'onglet **Arborescence**, cliquez sur **Packages**.

5. Dans le menu **Action**, cliquez sur **Nouveau** > **Pack à partir d'une définition**.

   L'écran **Bienvenue** de l'**Assistant Création de lot à partir d'une définition** apparaît.

6. Cliquez sur **Suivant**.

   L'écran **Définition du pack** apparaît.

7. Cliquez sur **Parcourir**.

   L'écran **Ouvrir** apparaît.

8. Recherchez le fichier de pack MSI. Le fichier se trouve sur le dossier partagé que vous avez créé.

9. Cliquez sur **Suivant**.

   L'écran **Fichiers sources** apparaît.

10. Cliquez sur **Toujours obtenir les fichiers du répertoire source**, puis sur **Suivant**.

    L'écran **Dossier source** apparaît.

11. Cliquez sur **Chemin d’accès au réseau (nom UNC)**.

12. Cliquez sur **Parcourir** et sélectionnez le répertoire source contenant le fichier MSI (dossier partagé précédemment créé).

13. Cliquez sur **Suivant**.

    L'assistant crée le pack. Une fois le processus terminé, le nom du pack apparaît sur la console **Administrateur SMS**.

Distribution du package à des endpoints cibles

Procédure

1. Sous l'onglet **Arborescence**, cliquez sur **Publications**.

2. Dans le menu **Action**, cliquez sur **Toutes les tâches** > **Distribuer le programme**.

   L'écran **Bienvenue** de l'**assistant de distribution** apparaît.

3. Cliquez sur **Suivant**.

   L’écran **Pack** apparaît.

4. Cliquez sur **Sélectionner un package existant**, puis sur le nom du pack d'installation que vous avez créé.

5. Cliquez sur **Suivant**.

   L’écran **Points de distribution** apparaît.

6. Sélectionnez le point de distribution vers lequel vous souhaitez copier le pack, puis cliquez sur **Suivant**.

   L’écran **Publier un programme** apparaît.

7. Cliquez sur **Oui** pour publier le nouveau package d'installation de l'agent OfficeScan, puis cliquez sur **Suivant**.

   L’écran **Cible de la publication** apparaît.

8. Cliquez sur **Parcourir** pour sélectionner les ordinateurs cibles.

L’écran **Parcourir le regroupement** apparaît.

9. Cliquez sur **Tous les systèmes Windows NT**.

10. Cliquez sur **OK**.

    L’écran **Cible de la publication** apparaît à nouveau.

11. Cliquez sur **Suivant**.

    L’écran **Nom de la publication** apparaît.

12. Dans les zones de texte, entrez un nom et vos remarques concernant la publication, puis cliquez sur **Suivant**.

    L’écran **Publier dans sous-groupes** apparaît.

13. Décidez si l'annonce du nouveau pack doit ou non s'adresser aux sous-groupes. Choisissez de publier ce programme uniquement pour les membres du groupe indiqué ou pour les membres du sous-groupe.

14. Cliquez sur **Suivant**.

    L’écran **Calendrier des publications** apparaît.

15. Indiquez à quel moment publier le package d'installation de l'agent OfficeScan. Pour cela, saisissez ou sélectionnez la date et l'heure.



Remarque

Si vous souhaitez que Microsoft SMS cesse la publication du pack à une date précise, cliquez sur **Oui. Cette publication doit expirer**. Ensuite, indiquez la date et l'heure dans les zones **Date et heure d'expiration**.

16. Cliquez sur **Suivant**.

    L’écran **Attribuer le programme** apparaît.

17. Cliquez sur **Oui, attribuer le programme**, puis cliquez sur **Suivant**.

    Microsoft SMS génère l'annonce et l'affiche sur la console Administrateur SMS.

18. Lorsque Microsoft SMS distribue aux ordinateurs cibles le programme oublié (en l'occurrence, le programme de l'agent OfficeScan), un écran s'affiche sur chacun de

ces endpoints. Demandez aux utilisateurs de cliquer sur **Oui** et de suivre les instructions fournies par l'assistant afin d'installer l'agent OfficeScan sur leur ordinateur.

Installations à partir d'une image disque d'un agent

La technologie de création d'image disque vous permet de créer l'image d'un agent OfficeScan à l'aide d'un logiciel de création d'image disque et de la cloner sur les autres ordinateurs du réseau.

Chaque installation d'un agent OfficeScan requiert un identificateur global unique (GUID) permettant au serveur d'identifier les agents individuellement. Utilisez le programme OfficeScan appelé `Imgsetup.exe` pour créer un GUID différent pour chaque clone.

Création d'une image disque de l'agent OfficeScan

Procédure

1. Installez l'agent OfficeScan sur le endpoint.
2. Copiez `ImgSetup.exe` depuis le répertoire <*dossier d'installation du serveur*> `\PCCSRV\Admin\Utility\ImgSetup` sur ce endpoint.
3. Exécutez ensuite le fichier `ImgSetup.exe` sur ce endpoint.

   Ceci crée une clé de registre `RUN` sous `HKEY_LOCAL_MACHINE`.
4. Créez une image disque de l'agent OfficeScan à l'aide du logiciel de création d'image disque.
5. Redémarrez le clone :

   `ImgSetup.exe` démarre automatiquement et crée une nouvelle valeur GUID. L'agent OfficeScan communique ce nouveau GUID au serveur, lequel crée alors un nouvel enregistrement pour le nouvel agent OfficeScan.



AVERTISSEMENT!

Pour éviter que deux ordinateurs ne portent le même nom dans la base de données OfficeScan, modifiez manuellement le nom de l'endpoint ou le nom de domaine de l'agent OfficeScan cloné.

Utilisation de Vulnerability Scanner

Vulnerability Scanner sert à détecter les solutions antivirus installées, à rechercher les ordinateurs non protégés sur votre réseau et à installer l'agent OfficeScan sur ces ordinateurs.

Éléments à prendre en compte lors de l'utilisation de Vulnerability Scanner

Pour déterminer si vous devez utiliser Vulnerability Scanner, tenez compte des points suivants :

- *Administration du réseau à la page 5-40*
- *Topologie et architecture du réseau à la page 5-41*
- *Spécifications logicielles/matérielles à la page 5-42*
- *Structure de domaines à la page 5-42*
- *Trafic réseau à la page 5-43*
- *Taille du réseau à la page 5-43*

Administration du réseau

TABLEAU 5-7. Administration du réseau

INSTALLATION	EFFICACITÉ DE VULNERABILITY SCANNER
Administration avec stratégie de sécurité stricte	Très efficace. Vulnerability Scanner signale si un logiciel antivirus est installé sur tous les ordinateurs.

INSTALLATION	EFFICACITÉ DE VULNERABILITY SCANNER
Responsabilité administrative distribuée sur des sites différents	Moyennement efficace
Administration centralisée	Moyennement efficace
Service externalisé	Moyennement efficace
Les utilisateurs administrent leurs propres ordinateurs	Inefficace. Du fait que Vulnerability Scanner scanne le réseau pour vérifier les installations antivirus, il n'est pas possible que les utilisateurs scannent leur propre ordinateur.

Topologie et architecture du réseau

TABLEAU 5-8. Topologie et architecture du réseau

INSTALLATION	EFFICACITÉ DE VULNERABILITY SCANNER
Site unique	Très efficace. Vulnerability Scanner vous permet de scanner un segment IP complet et d'installer facilement l'agent OfficeScan sur le réseau local.
Plusieurs sites avec connexion à haut débit	Moyennement efficace
Plusieurs sites avec connexion à bas débit	Inefficace. Vous devez exécuter Vulnerability Scanner sur chaque site et l'installation de l'agent OfficeScan doit être dirigée vers un serveur OfficeScan local.
Ordinateurs distants et isolés	Moyennement efficace

Spécifications logicielles/matérielles

Tableau 5-9. Spécifications logicielles/matérielles

Installation	Efficacité de Vulnerability Scanner
Systèmes d'exploitation basés sur Windows NT	Très efficace. Vulnerability Scanner peut facilement installer l'agent OfficeScan à distance sur les ordinateurs qui exécutent des systèmes d'exploitation basés sur Windows NT.
Systèmes d'exploitation mixtes	Moyennement efficace. Vulnerability Scanner peut uniquement effectuer l'installation sur les ordinateurs qui exécutent des systèmes d'exploitation basés sur Windows NT.
Logiciels de gestion des postes de travail	Inefficace. Vulnerability Scanner ne peut pas être utilisé avec les logiciels de gestion des postes de travail. Cependant, il permet de suivre l'avancement de l'installation de l'agent OfficeScan.

Structure de domaines

Tableau 5-10. Structure de domaines

Installation	Efficacité de Vulnerability Scanner
Microsoft Active Directory	Très efficace. Spécifiez le compte d'administrateur de domaine dans Vulnerability Scanner pour permettre l'installation à distance de l'agent OfficeScan.
Groupe de travail	Inefficace. Il se peut que Vulnerability Scanner ait difficultés à s'installer sur des ordinateurs utilisant des comptes d'administration et des mots de passe différents.
Novell™ Directory Service	Inefficace. Vulnerability Scanner nécessite un compte de domaine Windows pour installer l'agent OfficeScan.

INSTALLATION	EFFICACITÉ DE VULNERABILITY SCANNER
Peer To Peer	Inefficace. Il se peut que Vulnerability Scanner ait difficultés à s'installer sur des ordinateurs utilisant des comptes d'administration et des mots de passe différents.

Trafic réseau

TABLEAU 5-11. Trafic réseau

INSTALLATION	EFFICACITÉ DE VULNERABILITY SCANNER
Connexion en réseau local	Très efficace
512 Kbits/s	Moyennement efficace
Connexion T1 et supérieure	Moyennement efficace
RTC	Inefficace. L'installation de l'agent OfficeScan dure un certain temps.

Taille du réseau

TABLEAU 5-12. Taille du réseau

INSTALLATION	EFFICACITÉ DE VULNERABILITY SCANNER
Très grande entreprise	Très efficace. Plus le réseau est étendu, plus Vulnerability Scanner est nécessaire pour vérifier les installations de l'agent OfficeScan.
Petites et moyennes entreprises	Moyennement efficace. Pour les réseaux de petite taille, Vulnerability Scanner peut constituer une solution pour installer l'agent OfficeScan. Les autres méthodes d'installations de l'agent OfficeScan peuvent s'avérer beaucoup plus simples à mettre en œuvre.

Instructions pour l'installation de l'agent OfficeScan avec Vulnerability Scanner

Vulnerability Scanner n'installe pas l'agent OfficeScan si :

- Le serveur OfficeScan ou un autre logiciel de sécurité est installé sur l'ordinateur hôte cible.
- Le endpoint distant fonctionne sous Windows XP Édition Familiale, Windows Vista Édition Familiale Basique, Windows Vista Édition Familiale Premium, Windows 7 Édition Familiale Basique, Windows 7 Édition Familiale Premium, Windows 8 (versions basiques) ou Windows 8.1.



Remarque

Vous pouvez installer l'agent OfficeScan sur l'ordinateur hôte cible à l'aide des méthodes d'installation abordées dans la rubrique *Éléments à prendre en compte pour le déploiement à la page 5-11*.

Avant d'utiliser Vulnerability Scanner pour installer l'agent OfficeScan, procédez comme suit :

- Pour Windows Vista (Professionnel, Entreprise ou Édition intégrale), Windows 7 (Professionnel, Entreprise ou Édition intégrale), Windows 8 (Professionnel ou Entreprise), Windows 8.1 ou Windows Server 2012 (Standard) :
  1. Activez un compte administrateur intégré et définissez un mot de passe pour le compte.
  2. Cliquez sur **Démarrer** > **Tous les programmes** > **Outils administrateurs** > **Pare-feu Windows avec fonctions avancées de sécurité**.
  3. Pour Profil de domaine, Profil privé et Profil public, configurez l'état du pare-feu sur « Désactivé ».
  4. Ouvrez Microsoft Management Console (cliquez sur **Démarrer** > **Exécuter** et entrez `services.msc`) puis démarrez le service **Accès à distance au Registre**. Lors de l'installation de l'agent OfficeScan, utilisez le compte administrateur intégré et le mot de passe correspondant.
- Pour Windows XP Professionnel (versions 32 bits et 64 bits) :

1. Ouvrez l'Explorateur Windows et cliquez sur **Outils** > **Options des dossiers**.
2. Cliquez sur l'onglet **Affichage** et désactivez **Utiliser le partage de fichiers simple (recommandé)**.

Méthodes de vulnerability scan

Les scans de vulnérabilité vérifient la présence de logiciels de sécurité sur les ordinateurs hôtes et peut installer l'agent OfficeScan sur les ordinateurs non protégés.

Il existe plusieurs façons d'exécuter un vulnerability scan.

TABLEAU 5-13. Méthodes de vulnerability scan

MÉTHODE	DÉTAILS
Vulnerability scan manuel	Les administrateurs peuvent effectuer des scans de vulnérabilité sur demande.
Scan DHCP	Les administrateurs peuvent effectuer des scans de vulnérabilité sur des ordinateurs hôtes qui demandent des adresses IP à un serveur DHCP. Vulnerability Scanner écoute sur le port 67 qui est le port d'écoute du serveur DHCP pour les requêtes DHCP. S'il détecte une requête DHCP provenant d'un ordinateur hôte, un vulnerability scan s'exécute sur l'ordinateur. **Remarque** Vulnerability Scanner ne peut pas détecter de requêtes DHCP si vous l'avez exécuté sous Windows Server 2008, Windows 7, Windows 8, Windows 8.1 ou Windows Server 2012.
Vulnerability scan programmé	Des scans de vulnérabilité sont automatiquement exécutés en fonction du programme configuré par les administrateurs.

Une fois Vulnerability Scanner lancé, l'état de l'agent OfficeScan sur les ordinateurs hôtes cibles s'affiche. L'état peut être :

- **Normal** : l'agent OfficeScan est opérationnel et fonctionne correctement

- **Anormal** : les services de l'agent OfficeScan ne fonctionnent pas ou l'agent ne dispose pas de protection en temps réel
- **Non installé** : le service TMListen est manquant ou l'agent OfficeScan n'a pas été installé
- **Inaccessible** : Vulnerability Scanner n'a pas réussi à établir la connexion avec l'ordinateur hôte et à déterminer l'état de l'agent OfficeScan

Exécution d'un scan manuel de Vulnerability

Procédure

1. Pour effectuer un scan de vulnérabilité sur le serveur OfficeScan, accédez à <*Dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\TMVS`, puis double-cliquez sur `TMVS.exe`. La console Trend Micro Vulnerability Scanner apparaît. Pour effectuer un scan de vulnérabilité sur un autre endpoint fonctionnant sous Windows Server 2003, Server 2008, Vista, 7, 8, 8.1 ou Server 2012 :

    a. Sur l'ordinateur du serveur OfficeScan, accédez au répertoire `<dossier d'installation du serveur>\PCCSRV\Admin\Utility`.

    b. Copiez le dossier `TMVS` sur l'autre endpoint.

    c. Sur l'autre endpoint, ouvrez le dossier `TMVS` et double-cliquez sur `TMVS.exe`.

    La console **Trend Micro Vulnerability Scanner** apparaît.



Remarque

Vous ne pouvez pas lancer l'outil à partir de Terminal Server.

2. Rendez-vous à la section **Scan manuel**.

3. Saisissez la plage d'adresses IP des ordinateurs que vous souhaitez vérifier.

    a. Saisissez une plage d'adresses IPv4.



Remarque

Vulnerability Scanner peut uniquement effectuer des recherches dans une plage d'adresses IPv4 s'il est exécuté sur un ordinateur IPv4 pur ou à double-pile. Vulnerability Scanner prend uniquement en charge les plages d'adresses IP de la classe B, par exemple 168.212.1.1 à 168.212.254.254.

b. Pour une plage d'adresses IPv6, saisissez le préfixe IPv6 et la longueur du préfixe.



Remarque

Vulnerability Scanner peut uniquement effectuer des recherches dans une plage d'adresses IPv6 s'il est exécuté sur un ordinateur hôte IPv6 pur ou à double-pile.

4. Cliquez sur **Settings**.

   L'écran **Paramètres** apparaît.

5. Configurez les paramètres suivants :

   a. **Paramètres de ping** : Un scan de vulnérabilité peut envoyer des requêtes « ping » aux adresses IP spécifiées précédemment pour vérifier si elles sont en cours d'utilisation. Si un ordinateur hôte cible utilise une de ces adresses IP, Vulnerability Scanner peut déterminer le système d'exploitation de l'ordinateur hôte. Pour obtenir des informations détaillées, voir *Paramètres de ping à la page 5-61*.

   b. **Méthode de récupération des descriptions d'ordinateurs** : Vulnerability Scanner peut récupérer des informations complémentaires concernant les ordinateurs hôtes qui répondent à la commande « ping ». Pour obtenir des informations détaillées, voir *Méthode de récupération des descriptions des endpoints à la page 5-58*.

   c. **Recherche de produits** : Vulnerability Scanner peut vérifier la présence de logiciels de sécurité sur les ordinateurs hôtes cibles. Pour obtenir des informations détaillées, voir *Recherche de produits à la page 5-55*.

   d. **Paramètres du serveur OfficeScan** : configurez ces paramètres si vous souhaitez que Vulnerability Scanner installe automatiquement l'agent

OfficeScan sur les ordinateurs hôtes non protégés. Ces paramètres identifient le serveur parent de l'agent OfficeScan et les informations d'authentification d'administration utilisées pour se connecter aux ordinateurs hôtes. Pour obtenir des informations détaillées, voir *Paramètres du serveur OfficeScan à la page 5-63*.



Remarque

Certaines conditions peuvent empêcher l'installation de l'agent OfficeScan sur les ordinateurs hôtes cibles. Pour obtenir des informations détaillées, voir *Instructions pour l'installation de l'agent OfficeScan avec Vulnerability Scanner à la page 5-44*.

e. **Notifications** : Vulnerability Scanner peut envoyer les résultats de vulnerability scan aux administrateurs OfficeScan. Il peut également afficher des notifications sur les ordinateurs hôtes non protégés. Pour obtenir des informations détaillées, voir *Notifications à la page 5-59*.

f. **Enregistrer les résultats** : En plus d'envoyer les résultats du vulnerability scan aux administrateurs, Vulnerability Scanner peut également enregistrer les résultats du scan dans un fichier `.csv`. Pour obtenir des informations détaillées, voir *Résultats de Vulnerability Scan à la page 5-60*.

6. Cliquez sur **OK**.

L'écran Paramètres se ferme.

7. Cliquez sur **Start**.

Les résultats du scan des failles s'affichent dans le tableau **Résultats** sous l'onglet **Scan manuel**.



Remarque

Les informations relatives à l'adresse MAC ne s'affichent pas dans le tableau **Résultats** si le endpoint exécute Windows Server 2008 ou Windows Server 2012.

8. Pour enregistrer les résultats dans un fichier au format CSV (valeurs séparées par des virgules), cliquez sur **Exporter**, localisez le dossier dans lequel vous voulez enregistrer le fichier, tapez le nom du fichier et cliquez sur **Enregistrer**.

Exécution d'un scan DHCP

Procédure

1. Configurez les paramètres DHCP dans le fichier `TMVS.ini` qui se trouve dans le dossier suivant : <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\TMVS`.

Tableau 5-14. Paramètres DHCP dans le fichier `TMVS.ini`

Paramètre	Description
DhcpThreadNum=x	Spécifiez le numéro de thread pour le mode DHCP. La valeur minimale est 3 et la valeur maximale 100. La valeur par défaut est 8.
DhcpDelayScan=x	Il s'agit du délai d'attente, en secondes, avant que ne soit vérifié sur le endpoint demandeur si le logiciel antivirus est installé. La valeur minimale est 0 (aucune attente) et la valeur maximale 600. La valeur par défaut est 30.
LogReport=x	0 désactive l'écriture dans le journal et 1 l'active. Vulnerability Scanner envoie les résultats du scan au serveur OfficeScan. Les journaux s'affichent dans l'écran **Journaux des événements du système** de la console Web.
OsceServer=x	Adresse IP ou nom DNS du serveur OfficeScan.
OsceServerPort=x	Port du serveur Web sur le serveur OfficeScan.

2. Pour exécuter un scan de vulnérabilité sur le serveur OfficeScan, accédez au `<dossier d'installation du serveur>\PCCSRV\Admin\Utility\TMVS`, puis double-cliquez sur `TMVS.exe`. La console **Trend Micro Vulnerability Scanner** apparaît.

    a. Sur l'ordinateur du serveur OfficeScan, accédez au répertoire `<dossier d'installation du serveur>\PCCSRV\Admin\Utility`.

    b. Copiez le dossier `TMVS` sur l'autre endpoint.

    c. Sur l'autre endpoint, ouvrez le dossier `TMVS` et double-cliquez sur `TMVS.exe`.

La console **Trend Micro Vulnerability Scanner** apparaît.



Remarque

Vous ne pouvez pas lancer l'outil à partir de Terminal Server.

3. Dans la section **Scan manuel**, cliquez sur **Paramètres**.

   L'écran **Paramètres** apparaît.

4. Configurez les paramètres suivants :

   a. **Recherche de produits** : Vulnerability Scanner peut vérifier la présence de logiciels de sécurité sur les ordinateurs hôtes cibles. Pour obtenir des informations détaillées, voir *Recherche de produits à la page 5-55*.

   b. **Paramètres du serveur OfficeScan** : configurez ces paramètres si vous souhaitez que Vulnerability Scanner installe automatiquement l'agent OfficeScan sur les ordinateurs hôtes non protégés. Ces paramètres identifient le serveur parent de l'agent OfficeScan et les informations d'authentification d'administration utilisées pour se connecter aux ordinateurs hôtes. Pour obtenir des informations détaillées, voir *Paramètres du serveur OfficeScan à la page 5-63*.

   Remarque

   Certaines conditions peuvent empêcher l'installation de l'agent OfficeScan sur les ordinateurs hôtes cibles. Pour obtenir des informations détaillées, voir *Instructions pour l'installation de l'agent OfficeScan avec Vulnerability Scanner à la page 5-44*.

   c. **Notifications** : Vulnerability Scanner peut envoyer les résultats de vulnerability scan aux administrateurs OfficeScan. Il peut également afficher des notifications sur les ordinateurs hôtes non protégés. Pour obtenir des informations détaillées, voir *Notifications à la page 5-59*.

   d. **Enregistrer les résultats** : En plus d'envoyer les résultats du vulnerability scan aux administrateurs, Vulnerability Scanner peut également enregistrer les résultats du scan dans un fichier `.csv`. Pour obtenir des informations détaillées, voir *Résultats de Vulnerability Scan à la page 5-60*.

5. Cliquez sur **OK**.

   L'écran Paramètres se ferme.

6. Dans la table **Résultats**, cliquez sur l'onglet **Scan DHCP**.



Remarque

L'onglet **Scan DHCP** n'est pas disponible sur les ordinateurs exécutant Windows Server 2008, Windows 7, Windows 8, Windows 8.1 et Windows Server 2012.

7. Cliquez sur **Start**.

   Vulnerability scanner commence à écouter les requêtes DHCP et à exécuter les contrôles de failles sur les ordinateurs au fur et à mesure qu'ils se connectent au réseau.

8. Pour enregistrer les résultats dans un fichier au format CSV (valeurs séparées par des virgules), cliquez sur **Exporter**, localisez le dossier dans lequel vous voulez enregistrer le fichier, tapez le nom du fichier et cliquez sur **Enregistrer**.

Configuration d'un scan Vulnerability programmé

Procédure

1. Pour effectuer un scan de vulnérabilité sur le serveur OfficeScan, accédez à <*Dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\TMVS`, puis double-cliquez sur `TMVS.exe`. La console **Trend Micro Vulnerability Scanner** apparaît. Pour effectuer un scan de vulnérabilité sur un autre endpoint fonctionnant sous Windows Server 2003, Server 2008, Vista, 7, 8, 8.1 ou Server 2012 :

   a. Sur l'ordinateur du serveur OfficeScan, accédez au répertoire `<dossier d'installation du serveur>\PCCSRV\Admin\Utility`.

   b. Copiez le dossier `TMVS` sur l'autre endpoint.

   c. Sur l'autre endpoint, ouvrez le dossier `TMVS` et double-cliquez sur `TMVS.exe`.

      La console **Trend Micro Vulnerability Scanner** apparaît.



Remarque

Vous ne pouvez pas lancer l'outil à partir de Terminal Server.

2. Rendez-vous à la section **Scan programmé**.

3. Cliquez sur **Ajouter/Modifier**.

   L'écran **Scan programmé** apparaît.

4. Configurez les paramètres suivants :

   a. **Nom** : Saisissez le nom du scan de vulnérabilité programmé.

   b. **Plage d'adresses IP** : Saisissez la plage d'adresses IP des ordinateurs que vous souhaitez vérifier.

      i. Saisissez une plage d'adresses IPv4.

      Remarque

      Vulnerability Scanner peut uniquement effectuer des recherches dans une plage d'adresses IPv4 s'il est exécuté sur un ordinateur hôte IPv4 pur ou à double pile qui a une adresse IPv4 disponible. Vulnerability Scanner prend uniquement en charge les plages d'adresses IP de la classe B, par exemple 168.212.1.1 à 168.212.254.254.

      ii. Pour une plage d'adresses IPv6, saisissez le préfixe IPv6 et la longueur du préfixe.

      Remarque

      Vulnerability Scanner peut uniquement effectuer des recherches dans une plage d'adresses IPv6 s'il est exécuté sur un ordinateur hôte IPv6 pur ou à double pile qui a une adresse IPv6 disponible.

   c. **Programmation** : Spécifiez l'heure de début en utilisant le format 24 heures, puis sélectionnez la fréquence des scans. Choisissez s'il doit être quotidien, hebdomadaire ou mensuel.

   d. **Paramètres** : Sélectionnez quel ensemble de paramètres de scan de vulnérabilité utiliser.

- Sélectionnez **Utiliser les paramètres en cours** si vous avez configuré les paramètres de vulnerability scan manuel et que vous souhaitez les utiliser. Pour plus de détails sur les paramètres de vulnerability scan manuel, voir *Exécution d'un scan manuel de Vulnerability à la page 5-46*.
- Si vous n'avez pas spécifié de paramètres de vulnerability scan manuel ou que vous souhaitez utiliser un autre ensemble de paramètres, sélectionnez **Modifier les paramètres**, puis cliquez sur **Paramètres**. L'écran **Paramètres** apparaît.

  Vous pouvez configurer les paramètres suivants, puis cliquez sur **OK** :

  - **Paramètres de ping** : Un vulnerability scan peut envoyer des requêtes « ping » aux adresses IP spécifiées à l'étape 4b pour vérifier si elles sont en cours d'utilisation. Si un ordinateur hôte cible utilise une de ces adresses IP, Vulnerability Scanner peut déterminer le système d'exploitation de l'ordinateur hôte. Pour obtenir des informations détaillées, voir *Paramètres de ping à la page 5-61*.
  - **Méthode de récupération des descriptions d'ordinateurs** : Vulnerability Scanner peut récupérer des informations complémentaires concernant les ordinateurs hôtes qui répondent à la commande « ping ». Pour obtenir des informations détaillées, voir *Méthode de récupération des descriptions des endpoints à la page 5-58*.
  - **Recherche de produits** : Vulnerability Scanner peut vérifier la présence de logiciels de sécurité sur les ordinateurs hôtes cibles. Pour obtenir des informations détaillées, voir *Recherche de produits à la page 5-55*.
  - **Paramètres du serveur OfficeScan** : configurez ces paramètres si vous souhaitez que Vulnerability Scanner installe automatiquement l'agent OfficeScan sur les ordinateurs hôtes non protégés. Ces paramètres identifient le serveur parent de l'agent OfficeScan et les informations d'authentification d'administration utilisées pour se connecter aux ordinateurs hôtes. Pour obtenir des informations détaillées, voir *Paramètres du serveur OfficeScan à la page 5-63*.



Remarque

Certaines conditions peuvent empêcher l'installation de l'agent OfficeScan sur les ordinateurs hôtes cibles. Pour obtenir des informations détaillées, voir *Instructions pour l'installation de l'agent OfficeScan avec Vulnerability Scanner à la page 5-44*.

- **Notifications** : Vulnerability Scanner peut envoyer les résultats de vulnerability scan aux administrateurs OfficeScan. Il peut également afficher des notifications sur les ordinateurs hôtes non protégés. Pour obtenir des informations détaillées, voir *Notifications à la page 5-59*.

- **Enregistrer les résultats** : En plus d'envoyer les résultats du vulnerability scan aux administrateurs, Vulnerability Scanner peut également enregistrer les résultats du scan dans un fichier .csv. Pour obtenir des informations détaillées, voir *Résultats de Vulnerability Scan à la page 5-60*.

5. Cliquez sur **OK**.

   L'écran **Scan programmé** se ferme. Le vulnerability scan programmé que vous avez créé apparaît sous la section **Scan programmé**. Si vous avez activé les notifications, Vulnerability Scanner vous envoie les résultats du vulnerability scan programmé.

6. Pour exécuter immédiatement le vulnerability scan programmé, cliquez sur **Exécuter maintenant**.

   Les résultats du vulnerability scan s'affichent dans le tableau **Résultats** sous l'onglet **Scan programmé**.



Remarque

Les informations relatives à l'adresse MAC ne s'affichent pas dans le tableau **Résultats** si le endpoint exécute Windows Server 2008 ou Windows Server 2012.

7. Pour enregistrer les résultats dans un fichier au format `CSV` (valeurs séparées par des virgules), cliquez sur **Exporter**, localisez le dossier dans lequel vous voulez enregistrer le fichier, tapez le nom du fichier et cliquez sur **Enregistrer**.

Paramètres de Vulnerability Scan

La configuration des paramètres de vulnerability scan s'effectue à partir de Trend Micro Vulnerability Scanner (`TMVS.exe`) ou du fichier `TMVS.ini`.



Remarque

Reportez-vous à *Journaux de débogage du serveur à l'aide de LogServer.exe à la page 16-3* pour savoir comment collecter des journaux pour Vulnerability Scanner.

Recherche de produits

Vulnerability Scanner peut vérifier la présence de logiciels de sécurité sur les agents. Le tableau suivant explique comment Vulnerability Scanner vérifie la présence de produits de sécurité :

Tableau 5-15. Produits de sécurité vérifiés par Vulnerability Scanner

Produit	Description
ServerProtect for Windows	Vulnerability Scanner utilise le endpoint RPC pour vérifier si `SPNTSVC.exe` est en cours d'exécution. Il renvoie des informations telles que le système d'exploitation, le moteur de scan antivirus, le fichier de signatures de virus et les versions du produit. Vulnerability Scanner ne peut pas détecter le serveur d'informations ServerProtect ou la console de gestion ServerProtect.
ServerProtect for Linux	Si le endpoint cible n'exécute pas Windows, Vulnerability Scanner vérifie si ServerProtect for Linux est installé sur celui-ci en essayant de se connecter au port 14942.
agent OfficeScan	Vulnerability Scanner utilise le port de l'agent OfficeScan pour vérifier si l'agent OfficeScan est installé. Il vérifie également si le processus `TmListen.exe` est en cours d'exécution. Il extrait automatiquement le numéro de port s'il est exécuté à partir de son emplacement par défaut. Si vous avez lancé Vulnerability Scanner sur un endpoint autre que le serveur OfficeScan, vérifiez puis utilisez le port de communication de l'autre endpoint.

Produit	Description
PortalProtect™	Vulnerability Scanner charge la page Web `http://localhost:port/PortalProtect/index.html` afin de vérifier l'installation du produit.
ScanMail™ for Microsoft Exchange™	Vulnerability Scanner charge la page Web `http://ipaddress:port/scanmail.html` afin de vérifier l'installation de ScanMail.. Par défaut, ScanMail utilise le port 16372. Si ScanMail utilise un autre numéro de port, spécifiez-le. Sinon, Vulnerability Scanner ne pourra pas détecter ScanMail.
Gamme™ InterScan	Vulnerability Scanner charge les pages Web de différents produits pour vérifier leur installation. • InterScan Messaging Security Suite 5.x : `http://localhost:port/eManager/cgi-bin/eManager.htm` • InterScan eManager 3.x : `http://localhost:port/eManager/cgi-bin/eManager.htm` • InterScan VirusWall™ 3.x: `http://localhost:port/InterScan/cgi-bin/interscan.dll`
Trend Micro Internet Security™ (PC-cillin)	Vulnerability Scanner utilise le port 40116 pour vérifier si Trend Micro Internet Security est installé.
McAfee VirusScan ePolicy Orchestrator	Vulnerability Scanner envoie un jeton spécial au port TCP 8081, le port par défaut de ePolicy Orchestrator, pour fournir la connexion entre le serveur et l'agent. Le endpoint possédant ce produit antivirus répond en utilisant un type de jeton spécial. Vulnerability Scanner ne peut pas détecter la version autonome de McAfee VirusScan.
Norton Antivirus™ Corporate Edition	Vulnerability Scanner envoie un jeton spécial au port UDP port 2967, le port par défaut de Norton Antivirus Corporate Edition RTVScan. Le endpoint possédant ce produit antivirus répond en utilisant un type de jeton spécial. Comme Norton Antivirus Corporate Edition communique via UDP, le taux de précision n'est pas garanti. De plus, le trafic réseau peut influer sur le temps d'attente UDP.

Vulnerability Scanner détecte les produits et les ordinateurs à l'aide des protocoles suivants :

- **RPC**: pour détecter ServerProtect for NT.
- **UDP**: pour détecter les clients de Norton AntiVirus Corporate Edition.
- **TCP**: pour détecter McAfee VirusScan ePolicy Orchestrator.
- **ICMP**: pour détecter les ordinateurs en envoyant les paquets ICMP.
- **HTTP** : pour détecter les agents OfficeScan.
- **DHCP**: s'il détecte une requête DHCP, Vulnerability Scanner vérifie si un logiciel antivirus a déjà été installé sur le endpoint demandeur.

Configuration des paramètres Product Query

Les paramètres de recherche de produits sont un sous-ensemble des paramètres de vulnerability scan. Pour plus de détails sur les paramètres de vulnerability scan, voir *Méthodes de vulnerability scan à la page 5-45*.

Procédure

1. Pour définir les paramètres de recherche de produits à partir de Vulnerability Scanner (`TMVS.exe`) :
   a. Exécutez `TMVS.exe`.
   b. Cliquez sur **Settings**.

      L'écran **Paramètres** apparaît.
   c. Rendez-vous à la section **Recherche de produit**.
   d. Sélectionnez les produits à vérifier.
   e. Cliquez sur **Paramètres** en regard du nom d'un produit, puis spécifiez le numéro de port qui sera vérifié par Vulnerability Scanner.
   f. Cliquez sur **OK**.

      L'écran **Paramètres** se ferme.
2. Pour définir le nombre d'ordinateurs que Vulnerability Scanner vérifie simultanément à la recherche d'un programme antivirus :

a. Accédez au répertoire <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\TMVS` et ouvrez le fichier `TMVS.ini` à l'aide d'un éditeur de texte tel que le Bloc-notes.

b. Pour définir le nombre d'ordinateurs vérifiés lors de scans de vulnérabilité manuels, modifiez la valeur `ThreadNumManual`. Indiquez une valeur comprise entre 8 et 64.

   Saisissez par exemple `ThreadNumManual=60` pour que Vulnerability Scanner vérifie 60 ordinateurs en même temps.

c. Pour définir le nombre d'ordinateurs vérifiés lors de scans de vulnérabilité programmés, modifiez la valeur `ThreadNumSchedule`. Indiquez une valeur comprise entre 8 et 64.

   Saisissez par exemple `ThreadNumSchedule=50` pour que Vulnerability Scanner vérifie 50 ordinateurs en même temps.

d. Enregistrez le fichier `TMVS.ini`.

Méthode de récupération des descriptions des endpoints

Losrque Vulnerability Scanner est est mesure d'envoyer une requête « ping » aux ordinateurs hôtes, il peut récupérer des informations complémentaires concernant les ordinateurs hôtes. Il existe deux méthodes de récupération des informations :

- **Récupération rapide** : ne récupère que le nom de l'endpoint
- **Récupération normale** : récupère à la fois les informations relatives au domaine et au endpoint

Configuration des paramètres de récupération

Les paramètres de récupération sont un sous-ensemble des paramètres de vulnerability scan. Pour plus de détails sur les paramètres de vulnerability scan, voir *Méthodes de vulnerability scan à la page 5-45*.

Procédure

1. Exécutez `TMVS.exe`.

2. Cliquez sur **Settings**.

   L'écran **Paramètres** apparaît.

3. Rendez-vous à la section **Méthode de récupération des descriptions d'ordinateurs**.

4. Sélectionnez **Normale** ou **Rapide**.

5. Si vous avez sélectionné **Normal**, sélectionnez **Récuperer les descriptions d'ordinateurs si elles sont disponibles**.

6. Cliquez sur **OK**.

   L'écran **Paramètres** se ferme.

Notifications

Vulnerability Scanner peut envoyer les résultats de vulnerability scan aux administrateurs OfficeScan. Il peut également afficher des notifications sur les ordinateurs hôtes non protégés.

Configuration des paramètres de notification

Les paramètres de notification sont un sous-ensemble des paramètres de vulnerability scan. Pour plus de détails sur les paramètres de vulnerability scan, voir *Méthodes de vulnerability scan à la page 5-45*.

Procédure

1. Exécutez `TMVS.exe`.

2. Cliquez sur **Settings**.

   L'écran **Paramètres** apparaît.

3. Rendez-vous à la section **Notifications**.

4. Pour envoyer automatiquement les résultats de vulnerability scan à vous-même ou à d'autres administrateurs de votre entreprise :

a. Sélectionnez **Envoyer les résultats par courrier électronique à l'administrateur système**.

b. Cliquez sur **Configurer** pour spécifier les paramètres de courrier électronique.

c. Saisissez l'adresse e-mail du destinataire dans **À**.

d. Saisissez l'adresse e-mail de l'expéditeur dans **De**.

e. Entrez l'adresse du serveur SMTP dans **Serveur SMTP**.

   Saisissez par exemple `société.smtp.com`. Les informations relatives au serveur SMTP sont obligatoires.

f. Sous **Objet**, entrez un nouvel objet pour le message ou acceptez l'objet par défaut.

g. Cliquez sur **OK**.

5. Pour informer les utilisateurs que leurs ordinateurs n'ont aucun logiciel de sécurité installé :

a. Sélectionnez **Afficher une notification sur les ordinateurs non protégés**.

b. Cliquez sur **Personnaliser** pour configurer le message de notification.

c. Dans l'écran **Message de notification**, entrez un nouveau message ou acceptez le message par défaut.

d. Cliquez sur **OK**.

6. Cliquez sur **OK**.

L'écran **Paramètres** se ferme.

Résultats de Vulnerability Scan

Vous pouvez configurer Vulnerability Scanner pour qu'il enregistre les résultats de vulnerability scan en tant que fichier CSV (valeurs séparées par des virgules).

Configuration des résultats de scan

Les paramètres de résultats de vulnerability scan sont un sous-ensemble des paramètres de vulnerability scan. Pour plus de détails sur les paramètres de vulnerability scan, voir *Méthodes de vulnerability scan à la page 5-45*.

Procédure

1. Exécutez `TMVS.exe`.
2. Cliquez sur **Settings**.

   L'écran **Paramètres** apparaît.
3. Rendez-vous à la section **Enregistrer les résultats**.
4. Sélectionnez **Enregistrer automatiquement les résultats dans un fichier CSV**.
5. Pour modifier le dossier d'enregistrement du fichier `CSV` :
   a. Cliquez sur **Parcourir**.
   b. Sélectionnez un dossier cible sur le endpoint ou sur le réseau.
   c. Cliquez sur **OK**.
6. Cliquez sur **OK**.

   L'écran **Paramètres** se ferme.

Paramètres de ping

Utilisez les paramètres de « ping » pour confirmer l'existence d'un ordinateur cible et déterminer son système d'exploitation. Si ces paramètres sont désactivés, Vulnerability Scanner scanne toutes les adresses IP dans la plage d'adresses IP (même celles qui ne sont utilisées sur aucun ordinateur), ce qui rend la tentative de scan plus longue qu'elle ne devrait l'être.

Configuration des paramètres Ping

Les paramètres de ping sont un sous-ensemble des paramètres de vulnerability scan. Pour plus de détails sur les paramètres de vulnerability scan, voir *Méthodes de vulnerability scan à la page 5-45*.

Procédure

1. Pour définir les paramètres de ping à partir de Vulnerability Scanner (`TMVS.exe`) :

    a. Exécutez `TMVS.exe`.

    b. Cliquez sur **Settings**.

    L'écran **Paramètres** apparaît.

    c. Rendez-vous à la section **Paramètres de ping**.

    d. Sélectionnez **Permettre à Vulnerability Scanner d'envoyer une requête ping aux ordinateurs du réseau pour vérifier leur état**.

    e. Acceptez ou modifiez les valeurs des champs **Taille des paquets** et **Expiration**.

    f. Sélectionnez **Détecter le type de SE par le système de reconnaissance de SE**.

    Si vous sélectionnez cette option, Vulnerability Scanner détermine si un ordinateur hôte fonctionne sous Windows ou sous un autre système d'exploitation. Pour des ordinateurs hôtes fonctionnant sous Windows, Vulnerability Scanner peut identifier la version de Windows.

    g. Cliquez sur **OK**.

    L'écran **Paramètres** se ferme.

2. Pour définir le nombre d'ordinateurs auquel Vulnerability Scanner envoie simultanément une requête ping :

    a. Accédez au répertoire <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\TMVS` et ouvrez le fichier `TMVS.ini` à l'aide d'un éditeur de texte tel que le Bloc-notes.

b. Modifiez la valeur d'`EchoNum`. Indiquez une valeur comprise entre 1 et 64.

   Saisissez par exemple `EchoNum=60` pour que Vulnerability Scanner envoie une requête ping à 60 ordinateurs en même temps.

c. Enregistrez le fichier `TMVS.ini`.

Paramètres du serveur OfficeScan

Les paramètres de serveur OfficeScan sont utilisés lorsque :

- Vulnerability Scanner installe l'agent OfficeScan sur les ordinateurs cibles non protégés. Les paramètres du serveur permettent à Vulnerability Scanner d'identifier le serveur parent de l'agent OfficeScan, ainsi que les informations d'authentification d'administration à utiliser lors de la connexion aux ordinateurs cibles.



Remarque

Certaines conditions peuvent empêcher l'installation de l'agent OfficeScan sur les ordinateurs hôtes cibles. Pour obtenir des informations détaillées, voir *Instructions pour l'installation de l'agent OfficeScan avec Vulnerability Scanner à la page 5-44*.

- Vulnerability Scanner envoie les journaux d'installation de l'agent au serveur OfficeScan.

Configuration des paramètres du serveur OfficeScan

Les paramètres de serveur OfficeScan sont un sous-ensemble des paramètres de vulnerability scan. Pour plus de détails sur les paramètres de vulnerability scan, voir *Méthodes de vulnerability scan à la page 5-45*.

Procédure

1. Exécutez `TMVS.exe`.
2. Cliquez sur **Settings**.

   L'écran **Paramètres** apparaît.
3. Rendez-vous à la section **Paramètres de serveur OfficeScan**.

4. Tapez le nom et le numéro de port du serveur OfficeScan.

5. Sélectionnez **Installer automatiquement l'agent OfficeScan sur les ordinateurs non protégés**.

6. Pour configurer les informations d'authentification d'administration :

   a. Cliquez sur **Installation du compte**.

   b. Sur l'écran **Informations de compte**, entrez un nom d'utilisateur et un mot de passe.

   c. Cliquez sur **OK**.

7. Sélectionnez **Envoi des journaux au serveur OfficeScan**.

8. Cliquez sur **OK**.

   L'écran **Paramètres** se ferme.

Installation avec la conformité à la sécurité

Vous pouvez installer des agents OfficeScan sur des ordinateurs appartenant aux domaines du réseau ou installer l'agent OfficeScan sur un endpoint cible en utilisant son adresse IP.

Avant d'installer l'agent OfficeScan, veuillez noter les points suivants :

Procédure

1. Notez les informations de connexion de chaque endpoint. OfficeScan vous invitera à les spécifier pendant l'installation.

2. L'agent OfficeScan ne sera pas installé sur un endpoint si :

   - Le serveur OfficeScan est installé sur ce endpoint.

   - Ce endpoint fonctionne sous Windows XP Édition Familiale, Windows Vista Édition Familiale Basique, Windows Vista Édition Familiale Premium, Windows 7™ Édition Starter, Windows 7 Édition Familiale Basique, Windows 7 Édition Familiale Premium, Windows 8 (versions basiques) et

Windows 8.1. Si vous disposez d'ordinateurs exécutant ces plates-formes, choisissez une autre méthode d'installation. Voir *Éléments à prendre en compte pour le déploiement à la page 5-11* pour plus d'informations.

3. Si le endpoint cible fonctionne sous Windows Vista (Professionnel, Entreprise ou Édition intégrale), Windows 7 (Professionnel, Entreprise ou Édition intégrale), Windows 8 (Professionnel ou Entreprise), Windows 8.1 ou Windows Server 2012 (Standard), effectuez la procédure suivante sur le endpoint :

   a. Activez un compte administrateur intégré et définissez un mot de passe pour le compte.

   b. Désactivez le pare-feu Windows.

   c. Cliquez sur **Démarrer** > **Tous les programmes** > **Outils administrateurs** > **Pare-feu Windows avec fonctions avancées de sécurité**.

   d. Pour Profil de domaine, Profil privé et Profil public, configurez l'état du pare-feu sur « Désactivé ».

   e. Ouvrez Microsoft Management Console (cliquez sur **Démarrer** > **Exécuter** et tapez `services.msc`) puis démarrez le service **Accès à distance au Registre**. Lors de l'installation de l'agent OfficeScan, utilisez le compte administrateur intégré et le mot de passe correspondant.

4. Si des programmes de sécurité des endpoints Trend Micro ou tiers sont installés sur le endpoint, vérifiez qu'OfficeScan peut les désinstaller automatiquement et les remplacer par l'agent OfficeScan. Pour obtenir la liste des logiciels de sécurité agents qu'OfficeScan désinstalle automatiquement, ouvrez les fichiers suivants dans le répertoire <*dossier d'installation du serveur*>`\PCCSRV\Admin`. Vous pouvez ouvrir ces fichiers à l'aide d'un éditeur de texte comme le Bloc-notes.

   - `tmuninst.ptn`
   - `tmuninst_as.ptn`

   Si les logiciels présents sur le endpoint cible ne sont pas inclus dans la liste, désinstallez-les d'abord manuellement. En fonction du processus de désinstallation des logiciels, le endpoint procédera ou non à un redémarrage après la désinstallation.

Installation de l'agent OfficeScan

Procédure

1. Accédez à **Évaluation** > **Endpoints non gérés**.
2. Cliquez sur **Installer** en haut de l'arborescence des agents.
    - Si une version antérieure de l'agent OfficeScan est déjà installée sur le endpoint et que vous cliquez sur **Installer**, l'installation sera ignorée et l'agent ne sera pas mis à niveau vers cette version. Pour mettre l'agent à niveau, un paramètre doit être désactivé.
        a. Accédez à **Agents** > **Gestion des agents**.
        b. Cliquez sur l'onglet **Paramètres** > **Privilèges et autres paramètres** > **Autres paramètres**.
        c. Désactivez l'option **Les agents OfficeScan peuvent mettre à jour les composants, mais ne peuvent pas mettre à niveau le programme de l'agent, ni déployer des correctifs de type hot fix**.
3. Spécifiez le compte de connexion de l'administrateur pour chaque endpoint et cliquez sur **Connexion**. OfficeScan lance l'installation de l'agent sur le endpoint cible.
4. Affichez l'état de l'installation.

Migration vers l'agent OfficeScan

Remplacez le logiciel de sécurité de l'agent installé sur un endpoint cible par l'agent OfficeScan.

Migration à partir d'autres logiciels de sécurité de endpoints

Lorsque vous installez l'agent OfficeScan, le programme d'installation recherche les logiciels de sécurité des endpoints Trend Micro ou tiers installés sur le endpoint cible. Le

programme d'installation peut désinstaller automatiquement ces logiciels et les remplacer par l'agent OfficeScan.

Pour obtenir la liste des logiciels de sécurité des endpoints qu'OfficeScan désinstalle automatiquement, ouvrez les fichiers suivants dans le répertoire <*dossier d'installation du serveur*>`\PCCSRV\Admin`. Ouvrez ces fichiers à l'aide d'un éditeur de texte comme le Bloc-notes.

- `tmuninst.ptn`
- `tmuninst_as.ptn`

Si les logiciels présents sur le endpoint cible ne sont pas inclus dans la liste, désinstallez-les d'abord manuellement. En fonction du processus de désinstallation des logiciels, le endpoint procédera ou non à un redémarrage après la désinstallation.

Problèmes de migration des agents OfficeScan

- Si la migration automatique d'un agent est réussie mais qu'un utilisateur rencontre un problème avec l'agent OfficeScan juste après l'installation, redémarrez le endpoint.
- Si le programme d'installation d'OfficeScan a installé l'agent OfficeScan sans avoir pu désinstaller l'autre logiciel de sécurité, des conflits entre les deux logiciels peuvent se produire. Désinstallez les deux logiciels, puis installez l'agent OfficeScan à l'aide de l'une des méthodes d'installation décrites dans *Éléments à prendre en compte pour le déploiement à la page 5-11*.

Migration depuis des serveurs ServerProtect Normal

L'outil ServerProtect™ Normal Server Migration est un outil qui vous aide à faire migrer vers l'agent OfficeScan les ordinateurs exécutant Trend Micro ServerProtect Normal Server.

L'outil ServerProtect Normal Server Migration possède les mêmes spécifications logicielles et matérielles que le serveur OfficeScan. Exécutez l'outil sur des ordinateurs équipés de Windows Server 2003 ou Windows Server 2008.

Une fois la désinstallation du serveur ServerProtect Normal exécutée, l'outil installe l'agent OfficeScan. Les paramètres de liste des exclusions de scan (pour tous les types de scan) sont également migrés vers l'agent OfficeScan.

Pendant l'installation de l'agent OfficeScan, le processus du programme d'installation de l'agent de l'outil de migration peut expirer, auquel cas le programme vous signale l'échec de l'installation. Toutefois, l'agent OfficeScan peut avoir été correctement installé. Vérifiez l'installation sur le endpoint de l'agent depuis la console Web OfficeScan.

La migration échoue dans les circonstances suivantes :

- L'agent distant ne dispose que d'une adresse IPv6. L'outil de migration ne prend pas en charge l'adressage IPv6.
- L'agent distant ne peut pas utiliser le protocole NetBIOS.
- Les ports 455, 337 et 339 sont bloqués
- L'agent distant ne peut pas utiliser le protocole RPC.
- Le service de registre distant est arrêté



Remarque

L'outil ServerProtect Normal Server Migration ne désinstalle pas l'agent Control Manager™ pour ServerProtect. Pour obtenir des instructions sur le mode de désinstallation de l'agent, consultez la documentation ServerProtect et/ou Control Manager.

Utilisation de l'outil ServerProtect Normal Server Migration

Procédure

1. Sur l'ordinateur du serveur OfficeScan, ouvrez le répertoire <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\SPNSXfr` et copiez les fichiers `SPNSXfr.exe` et `SPNSX.ini` dans le répertoire `<dossier d'installation du serveur>\PCCSRV\Admin`.

2. Cliquez deux fois sur le fichier `SPNSXfr.exe` pour ouvrir l'outil.

   La console de l'outil **Server Protect Normal Server Migration** s'ouvre.

3. Sélectionnez le serveur OfficeScan. Le chemin du serveur OfficeScan s'affiche sous le chemin du serveur OfficeScan. S'il est incorrect, cliquez sur **Parcourir** et sélectionnez le dossier `PCCSRV` du répertoire dans lequel vous avez installé OfficeScan. Pour permettre à l'outil de retrouver automatiquement le serveur OfficeScan lors de la prochaine ouverture de l'outil, cochez la case **Détection automatique du chemin du serveur** (cochée par défaut).

4. Sélectionnez les ordinateurs exécutant ServerProtect Normal Server sur lesquels effectuer la migration en cliquant l'une des options suivantes sous **Endpoint cible** :

   - **Arbre du réseau Windows** : affiche une arborescence des domaines du réseau. Pour sélectionner des ordinateurs à l'aide de cette méthode, cliquez sur les domaines dans lesquels rechercher les ordinateurs des agents.

   - **Nom du serveur d'informations** : effectue une recherche par nom de serveur d'informations. Pour sélectionner des ordinateurs à l'aide de cette méthode, saisissez le nom d'un serveur d'informations sur le réseau dans la zone de texte. Pour rechercher plusieurs serveurs d'informations, insérez un point-virgule « ; » entre les noms de serveurs.

   - **Nom précis du serveur habituel** : effectue une recherche par nom de serveur Normal Server. Pour sélectionner des ordinateurs à l'aide de cette méthode, saisissez le nom d'un serveur Normal Server sur le réseau dans la zone de texte. Pour rechercher plusieurs serveurs habituels, saisissez un point-virgule (;) entre les noms de serveurs.

   - **Recherche de la plage IP** : effectue une recherche par plage d'adresses IP. Pour sélectionner des ordinateurs à l'aide de cette méthode, saisissez une plage d'adresses IP de classe B sous IP range.



Remarque

Si un serveur DNS sur le réseau ne répond pas lorsque vous recherchez des agents, la recherche est bloquée. Attendez l'expiration du délai de recherche.

5. Sélectionnez **Redémarrer après l'installation** pour redémarrer automatiquement les ordinateurs cibles après la migration.

Il faut redémarrer les ordinateurs pour que la migration soit exécutée correctement. Si vous ne choisissez pas cette option, redémarrez manuellement les ordinateurs après la migration.

6. Cliquez sur **Rechercher**.

   Les résultats de la recherche s'affichent sous **ServerProtect Normal Servers**.

7. Cliquez sur les ordinateurs sur lesquels effectuer la migration.

   a. Pour sélectionner tous les ordinateurs, cliquez sur **Select All**.

   b. Pour désélectionner tous les ordinateurs, cliquez sur **Tout désélectionner**.

   c. Pour exporter la liste en tant que fichier CSV (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**.

8. Si la connexion sur les ordinateurs cibles requiert un nom d'utilisateur et un mot de passe, procédez comme suit :

   a. Cochez la case **Utiliser un mot de passe/compte de groupe**.

   b. Cliquez sur **Définir le compte de connexion**.

      L'écran Enter Administration Information s'affiche.

   c. Saisissez le nom d'utilisateur et le mot de passe.



Remarque

Utilisez le compte administrateur local/domaine pour vous connecter au endpoint cible. Si vous vous connectez avec des privilèges insuffisants, en tant qu'invité ou utilisateur normal par exemple, vous ne pourrez pas réaliser l'installation.

   d. Cliquez sur **OK**.

   e. Cliquez sur **Redemander si la connexion échoue** afin de pouvoir saisir de nouveau le nom d'utilisateur et le mot de passe durant le processus de migration si la connexion est impossible.

9. Cliquez sur **Migrer**.

10. Si vous n'avez pas sélectionné l'option **Redémarrer après l'installation** , redémarrez les ordinateurs pour compléter la migration.

Tâches après l'installation

Une fois l'installation effectuée, vérifiez les éléments suivants :

- *Raccourci de l'agent OfficeScan à la page 5-71*
- *Liste des programmes à la page 5-71*
- *Services de l'agent OfficeScan à la page 5-72*
- *Journaux d'installation de l'agent OfficeScan à la page 5-72*

Raccourci de l'agent OfficeScan

Les raccourcis de l'agent OfficeScan apparaissent dans le menu Démarrer de Windows sur le endpoint de l'agent.



FIGURE 5-2. Raccourci de l'agent OfficeScan

Liste des programmes

Security Agent se trouve dans la liste **Ajout/Suppression de programmes** du Panneau de configuration du endpoint de l'agent.

Services de l'agent OfficeScan

Les services suivants de l'agent OfficeScan s'affichent dans **Microsoft Management Console** :

- Service d'écoute d'OfficeScan NT (`TmListen.exe`)
- Service de scan en temps réel d'OfficeScanNT (`NTRtScan.exe`)
- Service proxy d'OfficeScan NT (`TmProxy.exe`)



Remarque

Le Service proxy d'OfficeScan NT n'existe pas sur les plates-formes Windows 8/8.1 et Windows Server 2012.

- Pare-feu d'OfficeScan NT (`TmPfw.exe`), si le pare-feu a été activé durant l'installation
- Service de prévention des modifications non autorisées de Trend Micro (`TMBMSRV.exe`)
- Structure de la solution client commune Trend Micro (`TmCCSF.exe`)

Journaux d'installation de l'agent OfficeScan

Le journal d'installation de l'agent OfficeScan, `OFCNT.LOG`, se trouve aux emplacements suivants :

- `%windir%` pour toutes les méthodes d'installation à l'exception de celle utilisant un pack MSI
- `%temp%` pour la méthode d'installation à l'aide du pack MSI

Tâches recommandées après l'installation

Trend Micro recommande d'effectuer les tâches suivantes après l'installation :

Mises à jour des composants

Mettez à jour les composants de l'agent OfficeScan afin de garantir la protection la plus à jour des agents contre les risques de sécurité. Vous pouvez effectuer manuellement des mises à jour sur les agents depuis la console Web ou demander aux utilisateurs d'exécuter l'option « Mettre à jour » depuis leurs ordinateurs.

Tester OfficeScan à l'aide du script de test EICAR

L'EICAR (European Institute for Computer Antivirus Research), institut européen pour la recherche sur les antivirus informatiques, a mis au point un script de test permettant de confirmer l'installation et la configuration appropriées du logiciel antivirus. Pour plus d'informations, consultez le site Web de l'EICAR :

http://www.eicar.org

Le script de test de l'EICAR est un fichier texte inerte qui porte l'extension `.com`. Il ne s'agit pas d'un virus et il ne contient aucun fragment de code viral mais la plupart des logiciels antivirus réagissent à sa présence comme s'il s'agissait d'un virus. Utilisez ce fichier pour simuler un incident viral et vérifier que les notifications par e-mail et les journaux de virus fonctionnent correctement.



AVERTISSEMENT!

N'utilisez jamais de véritables virus pour tester votre produit antivirus.

Exécution d'un test de scan

Procédure

1. Activez le scan en temps réel sur l'agent.
2. Copiez la chaîne de caractères suivante et collez-la dans un éditeur de texte tel que le Bloc-notes : `X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`
3. Enregistrez le fichier sous le nom `EICAR.com` dans un répertoire temporaire. OfficeScan détecte immédiatement le fichier.

4. Pour tester d'autres ordinateurs du réseau, joignez le fichier EICAR.com à un e-mail et envoyez-le à l'un des ordinateurs.



Conseil

Trend Micro vous recommande de compresser le fichier EICAR à l'aide d'un logiciel de compression tel que WinZip, puis d'effectuer un autre scan de test.

Désinstallation de l'agent OfficeScan

Il existe deux façons de désinstaller l'agent OfficeScan des ordinateurs :

- *Désinstallation de l'agent OfficeScan depuis la console Web à la page 5-74*
- *Exécution du programme de désinstallation de l'agent OfficeScan à la page 5-76*

Si vous ne parvenez pas à désinstaller l'agent OfficeScan à l'aide des méthodes ci-dessus, désinstallez-le manuellement. Pour obtenir des informations détaillées, voir *Désinstallation manuelle de l'agent OfficeScan à la page 5-77*.

Désinstallation de l'agent OfficeScan depuis la console Web

Désinstallez le programme de l'agent OfficeScan à partir de la console Web. N'effectuez la désinstallation que si vous rencontrez des problèmes avec le programme. Procédez immédiatement à la réinstallation afin d'assurer la continuité de la protection du endpoint contre les risques de sécurité.

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Tâches** > **Désinstallation de l'agent**.

4. Sur l'écran **Désinstallation de l'agent**, cliquez sur **Lancer la désinstallation**. Le serveur envoie une notification aux agents.

5. Vérifiez l'état de notification et assurez-vous que tous les agents ont reçu une notification.

   a. Cliquez sur **Sélectionner les endpoints n'ayant pas reçu de notification**, puis sur **Lancer la désinstallation** pour envoyer immédiatement une nouvelle notification aux agents n'ayant pas reçu de notification.

   b. Cliquez sur **Arrêter la désinstallation** pour qu'OfficeScan arrête d'envoyer des notifications aux agents recevant actuellement des notifications. Les agents ayant déjà reçu la notification et effectuant déjà la désinstallation ignorent cette commande.

Le programme de désinstallation de l'agent OfficeScan

Accordez aux utilisateurs le droit de désinstaller le programme de l'agent OfficeScan, puis demandez-leur d'exécuter le programme de désinstallation de l'agent depuis leur ordinateur.

Selon votre configuration, la désinstallation peut nécessiter un mot de passe. Si c'est le cas, veillez à partager le mot de passe uniquement avec les utilisateurs qui exécuteront le programme de désinstallation et à le modifier immédiatement s'il a été divulgué à d'autres utilisateurs.

Affectation du privilège de désinstallation de l'agent OfficeScan

---

Procédure

1. Accédez à **Agents** > **Gestion des agents**.

2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.

3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.

4. Dans l'onglet **Privilèges**, accédez à la section **Désinstallation**.

5. Pour autoriser la désinstallation sans mot de passe, sélectionnez **Autoriser les utilisateurs à désinstaller l'agent OfficeScan**. Si un mot de passe est nécessaire, sélectionnez **Demander un mot de passe aux utilisateurs lors de la désinstallation de l'agent OfficeScan**, saisissez un mot de passe et confirmez-le.

6. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :

   - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.

   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Exécution du programme de désinstallation de l'agent OfficeScan

---

Procédure

1. Dans le menu **Démarrer** de Windows, cliquez sur **Programmes** > **Trend Micro OfficeScan Agent** > **Désinstaller l'agent OfficeScan**.

   Vous pouvez également effectuer cette procédure :

   a. Cliquez **Panneau de configuration** > **Ajout/Suppression de programmes**.

   b. Sélectionnez **Trend Micro OfficeScan Agent** et cliquez sur **Modifier**.

   c. Suivez les instructions à l'écran.

2. Si vous y êtes invité, entrez le mot de passe de désinstallation. OfficeScan informe l'utilisateur sur la progression de la désinstallation et l'avertit lorsque celle-ci est

terminée. L'utilisateur n'a pas à redémarrer le endpoint de l'agent pour terminer la désinstallation.

Désinstallation manuelle de l'agent OfficeScan

Procédez à la désinstallation manuelle uniquement si vous rencontrez des problèmes pour désinstaller l'agent OfficeScan à partir de la console Web ou après avoir exécuté le programme de désinstallation.

Procédure

1. Connectez-vous au endpoint de l'agent à l'aide d'un compte disposant de privilèges d'administrateur.

2. Cliquez avec le bouton droit de la souris sur l'icône de l'agent OfficeScan dans la barre d'état système et sélectionnez **Décharger OfficeScan**. Si vous êtes invité à saisir un mot de passe, indiquez le mot de passe de déchargement, puis cliquez sur **OK**.

   Remarque

   - Pour Windows 8, 8.1 et Windows Server 2012, passez en mode Bureau pour décharger l'agent OfficeScan.

   - Désactivez le mot de passe sur les ordinateurs sur lesquels l'agent OfficeScan sera déchargé. Pour obtenir des informations détaillées, voir *Configuration des privilèges des agents et d'autres paramètres à la page 14-93*.

3. Si vous n'avez pas spécifié le mot de passe de déchargement, arrêtez les services suivants depuis Microsoft Management Console :

   - Service d'écoute d'OfficeScan NT
   - Pare-feu d'OfficeScan NT
   - Service de scan en temps réel d'OfficeScanNT
   - Service proxy d'OfficeScan NT



Remarque

Le Service proxy d'OfficeScan NT n'existe pas sur les plates-formes Windows 8, 8.1 et Windows Server 2012.

- Service de prévention des modifications non autorisées de Trend Micro
- Structure de la solution client commune Trend Micro

4. Supprimez le raccourci de l'agent OfficeScan du menu Démarrer.

- Sur Windows 8, 8.1 et Windows Server 2012 :

    a. Passez en mode Bureau.

    b. Déplacez le curseur de la souris dans le coin inférieur droit de l'écran et cliquez sur **Démarrer** dans le menu qui s'affiche.

    L'écran **Page d'accueil** apparaît.

    c. Cliquez avec le bouton droit de la souris sur **Trend Micro OfficeScan**.

    d. Cliquez sur **Détacher de l'écran d'accueil**.

- Sur toutes les autres plates-formes Windows :

    Cliquez sur **Démarrer** > **Programmes**, cliquez avec le bouton droit de la souris sur **Trend Micro OfficeScan Agent**, puis cliquez sur **Supprimer**.

5. Ouvrez l'éditeur de la base de registre (`regedit.exe`).



AVERTISSEMENT!

Cette procédure implique que vous supprimiez les clés de registre. Le fait d'apporter des modifications erronées à votre base de registre peut gravement affecter votre système. Effectuez toujours une copie sauvegarde avant de procéder à toute modification de la base de registre. Consultez l'aide de l'Éditeur du Registre pour obtenir des informations complémentaires.

6. Supprimez les clés de registre suivantes d'OfficeScan :

- Si aucun autre produit Trend Micro n'est installé sur le endpoint :

    - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro`

Pour les ordinateurs 64 bits :

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro

- Si d'autres produits Trend Micro sont installés sur le endpoint, supprimez uniquement les clés suivantes :
    - HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC
    - HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfcWatchDog

      Pour les ordinateurs 64 bits :

      HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\OfcWatchDog
    - HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp

      Pour les ordinateurs 64 bits :

      HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\PC-cillinNTCorp

7. Supprimez les clés/valeurs de registre suivantes :
    - Pour les systèmes 32 bits :
        - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\OfficeScanNT
        - Moniteur OfficeScanNT (REG_SZ) sous HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
    - Pour les systèmes 64 bits :
        - HKEY_LOCAL_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\OfficeScanNT
        - Moniteur OfficeScanNT (REG_SZ) sous HKEY_LOCAL_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows\CurrentVersion\Run
8. Supprimez toutes les instances des clés de registre suivantes aux emplacements ci-après :

- Emplacements :
  - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`
  - `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services`
  - `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services`
  - `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services`
- Clés :
  - NTRtScan
  - tmcfw
  - tmcomm
  - TmFilter
  - TmListen
  - tmpfw
  - TmPreFilter
  - TmProxy



Remarque

TmProxy n'existe pas sur les plates-formes Windows 8/8.1 et Windows Server 2012.

  - tmtdi



Remarque

tmtdi n'existe pas sur les plates-formes Windows 8/8.1 et Windows Server 2012.

  - VSApiNt
  - tmlwf (pour les ordinateurs fonctionnant sous Windows Vista/ Server 2008/Server 2012/Windows 7/8/8.1)

- tmwfp (pour les ordinateurs fonctionnant sous Windows Vista/ Server 2008/Server 2012/Windows 7/8/8.1)
- tmactmon
- TMBMServer
- TMebc
- tmevtmgr
- tmeevw (pour Windows 8/8.1/Server 2012)
- tmusa (pour Windows 8/8.1/Server 2012)
- tmnciesc
- tmeext (pour Windows XP/2003)

9. Fermez l'Éditeur du Registre.

10. Cliquez sur **Démarrer** > **Paramètres** > **Panneau de configuration** et double-cliquez sur **Système**.



Remarque

Pour les systèmes Windows 8/8.1 et Windows Server 2012, ignorez cette étape.

11. Cliquez sur l'onglet **Matériel**, puis sur **Gestionnaire de périphériques**.



Remarque

Pour les systèmes Windows 8/8.1 et Windows Server 2012, ignorez cette étape.

12. Cliquez sur **Affichage** > **Afficher les périphériques cachés**.



Remarque

Pour les systèmes Windows 8/8.1 et Windows Server 2012, ignorez cette étape.

13. Développez **Pilotes non-Plug and Play** et désinstallez les périphériques suivants (pour Windows XP/Vista/7/Server 2003/Server 2008) :

- tmcomm
- tmactmon
- tmevtmgr
- Trend Micro Filter
- Trend Micro PreFilter
- Trend Micro TDI Driver
- Trend Micro VSAPI NT
- Service de prévention des modifications non autorisées de Trend Micro
- Trend Micro WFP Callout Driver (pour les ordinateurs Windows Vista / Windows Server 2008 / 7)

14. Supprimez manuellement les pilotes Trend Micro à l'aide d'un éditeur de ligne de commande (Windows 8/8.1/Server 2012 uniquement) et des commandes suivantes :

- `sc delete tmcomm`
- `sc delete tmactmon`
- `sc delete tmevtmgr`
- `sc delete tmfilter`
- `sc delete tmprefilter`
- `sc delete tmwfp`
- `sc delete vsapint`
- `sc delete tmeevw`
- `sc delete tmusa`
- `sc delete tmebc`



Remarque

Exécutez l'éditeur de ligne de commande avec les privilèges d'administrateur (par exemple, effectuez un clic droit sur `cmd.exe` et cliquez sur **Exécuter en tant qu'administrateur**) afin de vous assurer que la commande est exécutée correctement.

15. Désinstallez le pilote du pare-feu commun.

    a. Cliquez avec le bouton droit de la souris sur **Emplacements de mon réseau** et cliquez sur **Propriétés**.

    b. Cliquez avec le bouton droit de la souris sur **Connexion au réseau local** et cliquez sur **Propriétés**.

    c. Dans l'onglet **Général**, sélectionnez **Pilote du pare-feu commun Trend Micro** et cliquez sur **Désinstaller**.

    Remarque

    Les étapes suivantes s'appliquent uniquement aux systèmes d'exploitation Windows Vista/Server 2008/Server 2012/Windows 7/8/8.1. Pour les agents utilisant tous les autres systèmes d'exploitation, passez à l'étape 15.

    d. Cliquez avec le bouton droit de la souris sur **Réseau** et cliquez sur **Propriétés**.

    e. Cliquez sur **Gérer les connexions réseau**.

    f. Cliquez avec le bouton droit de la souris sur **Connexion au réseau local** et cliquez sur **Propriétés**.

    g. Dans l'onglet **Réseau**, sélectionnez **Trend Micro NDIS 6.0 Filter Driver** et cliquez sur **Désinstaller**.

16. Redémarrez le endpoint de l'agent.

17. Si aucun autre produit Trend Micro n'est installé sur le endpoint, supprimez le répertoire d'installation `Trend Micro` (généralement `C:\Program Files \Trend Micro`). Pour les ordinateurs 64 bits, le dossier d'installation figure sous `C:\Program Files (x86)\Trend Micro`.

18. Si d'autres produits Trend Micro sont installés, supprimez les dossiers suivants :

- <*dossier d'installation de l'agent*>
- Le dossier `BM` sous le dossier d'installation Trend Micro (généralement, `C:\Program Files\Trend Micro\BM` pour les systèmes 32 bits et `C:\Program Files (x86)\Trend Micro\BM` pour les systèmes 64 bits)



Chapitre 6

Maintien d'une protection à jour

Ce chapitre décrit les composants de OfficeScan™Trend Micro™ et les procédures de mise à jour.

Les rubriques sont les suivantes :

Composants et programmes OfficeScan

OfficeScan utilise des composants et des programmes pour protéger les ordinateurs des agents contre les risques de sécurité les plus récents. Tenez ces composants et ces programmes à jour en exécutant des mises à jour manuelles ou programmées.

Outre les composants, les agents OfficeScan reçoivent également des fichiers de configuration mis à jour du serveur OfficeScan. Les agents ont besoin des fichiers de configuration pour appliquer les nouveaux paramètres. À chaque fois que vous modifiez les paramètres d'OfficeScan via la console Web, les fichiers de configuration sont modifiés.

Les composants sont regroupés de la façon suivante :

- *Composants de l'antivirus à la page 6-2*
- *Composants de Damage Cleanup Services à la page 6-7*
- *Composants du service Anti-spyware à la page 6-7*
- *Composants du pare-feu à la page 6-8*
- *Composant lié à la réputation de sites Web à la page 6-9*
- *Composants de surveillance des comportements à la page 6-9*
- *Programmes à la page 6-11*
- *Composants du service Connexions suspectes à la page 6-13*
- *Solution contre l'exploitation du navigateur à la page 6-14*

Composants de l'antivirus

Les composants d'antivirus comprennent les signatures, les pilotes et les moteurs suivants :

- *Fichiers de signatures de virus à la page 6-3*
- *Moteur de scan antivirus à la page 6-4*
- *Pilote de scan antivirus à la page 6-5*

- *Signatures IntelliTrap à la page 6-6*
- *Signatures d'exceptions IntelliTrap à la page 6-6*
- *Fichier de signatures d'inspection de la mémoire à la page 6-6*

Fichiers de signatures de virus

Le fichier de signatures de virus disponible sur le endpoint de l'agent dépend de la méthode de scan utilisée par l'agent. Pour plus d'informations sur les méthodes de scan, voir *Types de méthodes de scan à la page 7-9*.

TABLEAU 6-1. Fichiers de signatures de virus

MÉTHODE DE SCAN	FICHIER DE SIGNATURES UTILISÉ
Scan traditionnel	Le **Fichier de signatures de virus** contient des informations qui aident OfficeScan à identifier les virus ainsi que les programmes malveillants d'attaques mixtes les plus récents. Trend Micro crée et publie de nouvelles versions du fichier de signatures de virus plusieurs fois par semaine et chaque fois qu'un virus/programme malveillant particulièrement ravageur est détecté. Trend Micro vous conseille de programmer les mises à jour automatiques au moins toutes les heures. Cette fréquence est configurée par défaut sur tous les produits livrés.

Méthode de scan	Fichier de signatures utilisé
Smart Scan	En mode Smart Scan, les agents OfficeScan utilisent deux fichiers de signatures légers qui fonctionnent ensemble pour protéger de la même façon que les fichiers de signatures anti-programmes malveillants et anti-spyware conventionnels. Une source Smart Protection héberge le **Smart Scan Pattern** (fichier de signatures Smart Scan). Ce fichier de signatures est mis à jour toutes les heures et contient la majorité des définitions de signatures. Les agents Smart Scan ne téléchargent pas ce fichier de signatures. Les agents vérifient les menaces potentielles par rapport au fichier de signatures en envoyant des requêtes de scan à la source Smart Protection. La source de mise à jour de l'agent (serveur OfficeScan ou source de mise à jour personnalisée) héberge le fichier **Smart Scan Agent Pattern**. Ce fichier de signatures est mis à jour quotidiennement et contient toutes les autres définitions de signatures introuvables dans le Smart Scan Pattern. Les agents téléchargent ce fichier de signatures à partir de la source de mise à jour en utilisant la même méthode que pour le téléchargement des composants OfficeScan. Pour plus d'informations sur les fichiers Smart Scan Pattern et Smart Scan Agent Pattern, voir *Fichiers de signatures Smart Protection à la page 4-8*.

Moteur de scan antivirus

Au cœur de tous les produits Trend Micro se trouve le moteur de scan, initialement conçu pour faire face aux premiers fichiers viraux sur endpoints. Le moteur de scan actuel est exceptionnellement sophistiqué et capable de détecter différents types de *Virus et programmes malveillants à la page 7-2*. Le moteur de scan détecte également les virus sous contrôle conçus et utilisés pour la recherche.

Plutôt que de scanner chaque octet de chaque fichier, le moteur et le fichier de signatures collaborent à l'identification des éléments suivants :

- Caractéristiques révélatrices du code du virus
- Emplacement précis dans un fichier dans lequel se trouve le virus

OfficeScan supprime les virus/programmes malveillants détectés et restaure l'intégrité du fichier.

Mise à jour du moteur de scan

Grâce à l'enregistrement des informations de virus/programmes malveillants à durée de vie critique dans le fichier de signatures de virus, Trend Micro minimise le nombre de mises à jour du moteur de scan, tout en maintenant la protection à jour. Néanmoins, Trend Micro met régulièrement à disposition de nouvelles versions du moteur de scan. Trend Micro fournit de nouveaux moteurs dans les circonstances suivantes :

- Intégration de nouvelles technologies de scan et de détection au logiciel
- Découverte d'un nouveau virus/programme malveillant potentiellement dangereux que le moteur de scan n'est pas capable de traiter
- Optimisation des performances du scan
- Ajout de formats de fichiers, de langages de script, de formats de chiffrement et/ou de compression

Pilote de scan antivirus

Le pilote de scan antivirus contrôle les opérations de l'utilisateur sur les fichiers. Ces opérations incluent l'ouverture ou la fermeture des fichiers, ainsi que l'exécution d'une application. Il existe deux versions pour ce pilote. Il s'agit de `TmXPFlt.sys` et `TmPreFlt.sys`. `TmXPFlt.sys` est utilisé pour la configuration en temps réel du moteur de scan antivirus et `TmPreFlt.sys` pour le contrôle des opérations de l'utilisateur.



Remarque

Ce composant ne s'affiche pas sur la console. Pour vérifier la version, accédez au répertoire <*dossier d'installation du serveur*>`\PCCSRV\Pccnt\Drv`. Cliquez avec le bouton droit de la souris sur le fichier `.sys`, sélectionnez **Propriétés** et accédez à l'onglet **Version**.

Signatures IntelliTrap

Fichier de signatures d'IntelliTrap (pour plus d'informations, voir *IntelliTrap à la page E-7*). La signature détecte en temps réel les fichiers compressés en fichiers exécutables.

Signatures d'exceptions IntelliTrap

Le fichier de signatures d'exceptions IntelliTrap contient une liste des fichiers de compression « approuvés »

Fichier de signatures d'inspection de la mémoire

Le scan en temps réel utilise le fichier de signatures d'inspection de la mémoire pour évaluer les fichiers compressés exécutables identifiés par la surveillance des comportements. Le scan en temps réel effectue les actions suivantes sur les fichiers compressés exécutables :

1. Il crée un fichier mappage en mémoire après la vérification du chemin d'accès de l'image du processus.



Remarque

La liste des exclusions de scan a la priorité sur le scan de fichiers.

2. Il envoie l'ID du processus au service de protection avancé, qui effectue par la suite les actions suivantes :

    a. Il utilise le moteur de scan antivirus pour scanner la mémoire.

    b. Il filtre le processus à l'aide des listes globales d'éléments approuvés pour les fichiers système Windows, les fichiers signés numériquement provenant de sources fiables, ainsi que les fichiers testés par Trend Micro. S'il s'avère qu'un fichier est sans danger, OfficeScan n'exécute aucune action dessus.

3. Une fois le scan de la mémoire effectué, le service de protection avancé envoie les résultats au scan en temps réel.

4. Le scan en temps réel met alors en quarantaine tout programme malveillant détecté et met fin au processus.

Composants de Damage Cleanup Services

Les composants Damage Cleanup Services se composent du moteur et du modèle suivants.

- *Moteur de nettoyage de virus à la page 6-7*
- *Modèle de nettoyage de virus à la page 6-7*
- *Early Boot Clean Driver à la page 6-7*

Moteur de nettoyage de virus

Le Moteur de nettoyage de virus recherche et supprime les chevaux de Troie et leurs processus. Ce moteur est compatible avec les plates-formes 32 et 64 bits.

Modèle de nettoyage de virus

Le Modèle de nettoyage de virus est utilisé par le Moteur de nettoyage de virus pour identifier les fichiers et processus infestés de chevaux de Troie afin de les éliminer.

Early Boot Clean Driver

Le pilote Trend Micro Early Boot Clean Driver se charge avant ceux du système d'exploitation, ce qui lui permet de détecter et de bloquer les rootkits d'amorçage. Une fois l'agent OfficeScan chargé, le pilote Trend Micro Early Boot Clean Driver invoque Damage Cleanup Services pour nettoyer le rootkit.

Composants du service Anti-spyware

Les composants anti-spyware conprennent le moteur et les signatures suivants :

- *Signatures de spywares à la page 6-8*
- *Moteur de scan anti-spyware à la page 6-8*
- *Signatures de surveillance active des spywares à la page 6-8*

Signatures de spywares

Le Fichier de signatures de spywares identifie les spywares/graywares dans les fichiers et les programmes, les modules dans la mémoire, la base de registre de Windows et les raccourcis d'URL.

Moteur de scan anti-spyware

Le Moteur de scan anti-spyware recherche les spywares et les graywares, puis effectue l'action de scan appropriée. Ce moteur est compatible avec les plates-formes 32 et 64 bits.

Signatures de surveillance active des spywares

La signature de surveillance active des spywares est utilisée pour l'analyse anti-spyware et anti grayware en temps réel. Seuls les agents de scan traditionnel utilisent ce fichier de signatures.

Les agents Smart Scan utilisent le fichier Smart Scan Agent Pattern pour le scan anti-spyware et anti-grayware en temps réel. Les agents envoient des requêtes de scan à une source Smart Protection si le niveau de risque de la cible du scan ne peut pas être déterminé pendant le scan.

Composants du pare-feu

Les composants de pare-feu se composent du pilote et du fichier de signatures suivants :

- *Pilote du pare-feu commun à la page 6-8*
- *Signatures du pare-feu commun à la page 6-9*

Pilote du pare-feu commun

Le pilote du pare-feu commun est utilisé avec le fichier de signatures de pare-feu commun pour rechercher des virus de réseau sur les ordinateurs des agents. Ce pilote est compatible avec les plates-formes 32 et 64 bits.

Signatures du pare-feu commun

Tout comme le fichier de signatures de virus, le fichier de signatures du pare-feu commun aide OfficeScan à identifier les signatures de virus, signatures uniques des bits et des octets qui signalent la présence d'un virus de réseau.

Composant lié à la réputation de sites Web

Le composant lié à la réputation des sites Web est le Moteur de filtre URL.

Moteur de filtre URL

Le Moteur de filtre URL facilite la communication entre OfficeScan et le service de filtre d'URL de Trend Micro. Le service de filtre d'URL est un système qui évalue les URL et fournit des informations d'évaluation à OfficeScan.

Composants de surveillance des comportements

Les composants de surveillance des comportements se composent des signatures, pilotes et services suivants :

- *Signatures de détection de l'analyse comportementale à la page 6-9*
- *Pilote de surveillance des comportements à la page 6-10*
- *Service principal de surveillance des comportements à la page 6-10*
- *Modèle de configuration de la surveillance des comportements à la page 6-10*
- *Digital Signature Pattern à la page 6-10*
- *Modèle de conformité aux stratégies à la page 6-10*

Signatures de détection de l'analyse comportementale

Ce fichier de signatures contient les règles de détection des comportements de menaces suspects.

Pilote de surveillance des comportements

Ce pilote de noyau contrôle les événements système et les transmet au Service principal de surveillance des comportements pour l'application des stratégies.

Service principal de surveillance des comportements

Ce service en mode utilisateur offre les fonctions suivantes :

- Détection des rootkits
- Régulation de l'accès aux périphériques externes
- Protection des fichiers, des clés de registres et des services

Modèle de configuration de la surveillance des comportements

Le Pilote de la surveillance des comportements utilise ce fichier de signatures pour identifier les événements système normaux et les exclure de l'application des stratégies.

Digital Signature Pattern

Ce fichier de signatures contient la liste de signatures numériques valides utilisées par le Service principal de surveillance des comportements afin de déterminer si un programme responsable d'un événement système ne présente pas de danger.

Modèle de conformité aux stratégies

Le Service principal de surveillance des comportements vérifie les événements système et les compare aux stratégies de ce fichier de signatures.

Fichier de signatures de déclenchement du scan de la mémoire

La surveillance des comportements utilise le fichier de signatures de déclenchement du scan de la mémoire pour identifier des menaces potentielles lorsque les opérations suivantes ont été détectées :

- Action d'écriture dans un fichier.
- Action d'écriture dans une entrée de Registre.
- Création d'un processus.

Lorsque l'une de ces opérations est identifiée, la surveillance des comportements invoque le fichier de signatures d'inspection de la mémoire du scan en temps réel, afin de vérifier la présence de risques de sécurité.

Pour plus d'informations sur les opérations de scan en temps réel, voir *Fichier de signatures d'inspection de la mémoire à la page 6-6*.

Programmes

OfficeScan utilise les programmes et mises à jour des produits suivants :

- *Programme de l'agent OfficeScan à la page 6-11*
- *Correctifs de type hotfix, patchs et Service Packs à la page 6-11*

Programme de l'agent OfficeScan

Le programme de l'agent OfficeScan assure la protection effective contre les risques de sécurité.

Correctifs de type hotfix, patchs et Service Packs

Après la publication officielle d'un produit, Trend Micro développe souvent les éléments suivants afin de corriger les problèmes, d'améliorer les performances des produits ou d'y ajouter de nouvelles fonctionnalités.

- *Correctif de type hotfix à la page E-5*
- *Patch à la page E-10*
- *Correctif de sécurité à la page E-11*
- *Service Pack à la page E-12*

Votre revendeur ou votre service d'assistance technique peut vous contacter lorsque ces éléments sont disponibles. Consultez le site Web de Trend Micro pour obtenir des informations sur les nouveaux correctifs de type hotfix, patchs et service packs :

http://downloadcenter.trendmicro.com/index.php?regs=fr

Toutes les versions incluent un fichier Lisez-moi contenant des informations relatives à l'installation, au déploiement et à la configuration. Veuillez lire attentivement le fichier Lisez-moi avant d'exécuter l'installation.

Historique des correctifs de type hotfix et des patchs

Lorsque le serveur OfficeScan déploie des fichiers de correctifs de type hot fix ou de patchs sur les agents OfficeScan, le programme de l'agent enregistre des informations les concernant dans l'Éditeur de Registre. Vous pouvez lancer des requêtes sur ces informations pour plusieurs agents en utilisant des logiciels de logistique tels que Microsoft SMS, LANDesk™ ou BigFix™.



Remarque

Cette fonction n'enregistre pas les correctifs de type hot fix et les patchs qui ne sont déployés que sur le serveur.

Cette fonction est disponible à partir d'OfficeScan 8.0 Service Pack 1 avec le correctif 3,1.

- Les agents ayant été mis à niveau de la version 8.0 Service Pack 1 à l'aide du patch 3.1 ou ultérieur enregistrent les correctifs de type hot fix et les patchs installés pour les versions 8.0 et ultérieures.
- Les agents ayant été mis à niveau à partir des versions antérieures à la version 8.0 Service Pack 1 avec le patch 3.1 enregistrent les correctifs de type hot fix et les patchs installés pour les versions 10.0 et ultérieures.

Les informations sont stockées dans les clés suivantes :

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\HotfixHistory\<Product version>`
- Pour les ordinateurs exécutant les plates-formes x64 :

  `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\ PC-cillinNTCorp\CurrentVersion\HotfixHistory\<Product version>`

Recherchez les clés suivantes :

- **Clé** : `HotFix_installed`

  Type : `REG_SZ`

  Valeur : `<Nom du correctif de type hot fix ou du patch>`
- **Clé** : `HotfixInstalledNum`

  Type : `DWORD`

  Valeur : `<Numéro du correctif de type hot fix ou du patch>`

Composants du service Connexions suspectes

Les composants du service Connexions suspectes sont constitués de la liste et du fichier de signatures suivants :

- *Liste d'adresses IP C&C globale à la page 6-13*
- *Fichier de signatures de règle de pertinence à la page 6-14*

Liste d'adresses IP C&C globale

La liste d'adresses IP C&C globale fonctionne en binôme avec le moteur d'inspection du contenu réseau (NCIE) pour détecter les connexions réseaux avec des serveurs C&C connus. Le NCIE détecte un contact serveur C&C via n'importe quel canal réseau.

OfficeScan consigne dans des journaux toutes les informations de connexion à des serveurs de la liste d'adresses IP C&C globale pour évaluation.

Fichier de signatures de règle de pertinence

Le service Connexions suspectes utilise le fichier de signatures de règle de pertinence pour détecter des signatures uniques de familles de programmes malveillants au sein des en-têtes des paquets réseau.

Solution contre l'exploitation du navigateur

La solution contre l'exploitation du navigateur contient les fichiers de signatures suivants :

- *Fichier de signatures de prévention contre l'exploitation du navigateur à la page 6-14*
- *Fichier de signatures de l'analyseur de script à la page 6-14*

Fichier de signatures de prévention contre l'exploitation du navigateur

Ce fichier de signatures identifie les exploitations de navigateur Web les plus récentes et empêche leur utilisation.

Fichier de signatures de l'analyseur de script

Ce fichier de signatures analyse les scripts contenus dans les pages Web et identifie ceux considérés comme malveillants.

Présentation de la mise à jour

Toutes les mises à jour des composants proviennent du serveur Trend Micro ActiveUpdate Server. Lorsque des mises à jour sont disponibles, le serveur OfficeScan et les sources Smart Protection (Smart Protection Server ou Smart Protection Network) téléchargent les composants à jour. Il n'y a aucun risque de chevauchement de téléchargement de composants car les serveur OfficeScan et les sources Smart Protection téléchargent chacun un ensemble de composants spécifiques.



Remarque

Vous pouvez configurer le serveur OfficeScan et le serveur Smart Protection Server pour effectuer la mise à jour à partir d'une autre source que le serveur Trend Micro ActiveUpdate Server. Pour ce faire, vous devez définir une source de mise à jour personnalisée. Si vous avez besoin d'aide pour définir cette source de mise à jour, contactez votre service d'assistance.

Mise à jour du serveur OfficeScan et des agents OfficeScan

Le serveur OfficeScan télécharge la plupart des composants dont les agents ont besoin. Le seul composant qu'il ne télécharge pas est le fichier Smart Scan Pattern, qui est téléchargé par les sources Smart Protection.

Si un serveur OfficeScan gère un grand nombre d'agents, la mise à jour peut utiliser une quantité significative des ressources de l'ordinateur du serveur, ce qui nuit à la stabilité et aux performances de ce dernier. Pour résoudre ce problème, OfficeScan possède une fonction d'agent de mise à jour qui permet de répartir sur certains agents la tâche de distribution des mises à jour vers les autres agents.

Le tableau suivant décrit les différentes options de mise à jour des composants pour le serveur et les agents OfficeScan Server, ainsi que les recommandations d'utilisation :

Tableau 6-2. Options de mise à jour serveur-agents

Option de mise à jour	Description	Recommandation
Serveur ActiveUpdate > **Serveur** > **Agent**	Le serveur OfficeScan reçoit les composants mis à jour à partir du serveur ActiveUpdate de Trend Micro (ou d'une autre source de mise à jour) et lance la mise à jour des composants sur les agents.	Utilisez cette méthode s'il n'existe aucune section à faible bande passante entre les agents et le serveur OfficeScan.

OPTION DE MISE À JOUR	DESCRIPTION	RECOMMANDATION
Serveur ActiveUpdate > **Serveur** > **Agents de mise à jour** > **Agent**	Le serveur OfficeScan reçoit les composants mis à jour à partir du serveur ActiveUpdate (ou d'une autre source de mise à jour) et lance la mise à jour des composants sur les agents. Les agents agissant en tant qu'agent de mise à jour demandent ensuite aux agents de mettre à jour les composants.	Si votre réseau comporte des sections à faible bande passante situées entre les agents et le serveur OfficeScan, utilisez cette méthode pour équilibrer le volume du trafic sur le réseau.
Serveur ActiveUpdate > **Agents de mise à jour** > **Agent**	Les agents de mise à jour reçoivent les composants mis à jour directement à partir du serveur ActiveUpdate (ou d'une autre source de mise à jour) et demandent aux agents de mettre à jour les composants.	Utilisez cette méthode uniquement si vous rencontrez des difficultés pour mettre à jour les agents de mise à jour à partir du serveur OfficeScan ou des autres agents de mise à jour. Dans la majorité des cas, les agents de mise à jour reçoivent les mises à jour plus rapidement à partir du serveur OfficeScan ou des autres agents de mise à jour qu'à partir d'une source de mise à jour externe.
Serveur ActiveUpdate > **Agent**	Les agents OfficeScan reçoivent les composants mis à jour directement depuis le serveur ActiveUpdate (ou depuis une autre source de mise à jour).	Utilisez cette méthode uniquement si vous rencontrez des difficultés pour mettre à jour les agents à partir du serveur OfficeScan ou des agents de mise à jour. Dans la majorité des cas, les agents reçoivent les mises à jour plus rapidement à partir du serveur OfficeScan ou des agents de mise à jour qu'à partir d'une source de mise à jour externe.

Mise à jour des sources Smart Protection

Une source Smart Protection (Smart Protection Server ou Smart Protection Network) télécharge le Smart Scan Pattern. Les agents Smart Scan ne téléchargent pas ce fichier de signatures. Les agents vérifient les menaces potentielles par rapport au fichier de signatures en envoyant des requêtes de scan à la source Smart Protection.



Remarque

Consultez la rubrique *Sources Smart Protection à la page 4-6* pour obtenir de plus amples informations sur les sources Smart Protection.

Le tableau suivant décrit le processus de mise à jour pour les sources Smart Protection.

TABLEAU 6-3. Processus de mise à jour des sources Smart Protection

PROCESSUS DE MISE À JOUR	DESCRIPTION
Serveur ActiveUpdate > **Smart Protection Network**	Trend Micro Smart Protection Network reçoit les mises à jour du serveur Trend Micro ActiveUpdate Server. Les agents Smart Scan qui ne sont pas connectés au réseau d'entreprise envoient des requêtes à Trend Micro Smart Protection Network.
Serveur ActiveUpdate > **Smart Protection Server**	Un serveur Smart Protection Server (intégré ou autonome) reçoit les mises à jour du serveur Trend Micro ActiveUpdate. Les agents de Smart Protection qui sont connectés au réseau d'entreprise envoient des requêtes au serveur Smart Protection Server.
Smart Protection Network > **Smart Protection Server**	Un serveur Smart Protection Server (intégré ou autonome) reçoit les mises à jour de Trend Micro Smart Protection Network. Les agents de Smart Protection qui sont connectés au réseau d'entreprise envoient des requêtes au serveur Smart Protection Server.

Mises à jour du serveur OfficeScan

Le serveur OfficeScan télécharge les composants suivants et les déploie sur les agents :

Tableau 6-4. Composants téléchargés par le serveur OfficeScan

Composant	Distribution	
	Agents de scan traditionnel	Agents Smart Scan
Antivirus		
Smart Scan Agent Pattern	Non	Oui
Fichier de signatures de virus	Oui	Non
Signatures IntelliTrap	Oui	Oui
Signatures d'exceptions IntelliTrap	Oui	Oui
Fichier de signatures d'inspection de la mémoire	Oui	Oui
Moteur de scan antivirus (32 bits)	Oui	Oui
Moteur de scan antivirus (64 bits)	Oui	Oui
Anti-spyware		
Signatures de spywares	Oui	Oui
Signatures de surveillance active des spywares	Oui	Non
Moteur de scan anti-spyware (32 bits)	Oui	Oui
Moteur de scan anti-spyware (64 bits)	Oui	Oui
Damage Cleanup Services		
Modèle de nettoyage de virus	Oui	Oui
Moteur de nettoyage de virus (32 bits)	Oui	Oui
Moteur de nettoyage de virus (64 bits)	Oui	Oui
Early Boot Clean Driver (32 bits)	Oui	Oui
Early Boot Clean Driver (32 bits)	Oui	Oui

Composant	Distribution	
	Agents de scan traditionnel	Agents Smart Scan
Pare-feu		
Signatures du pare-feu commun	Oui	Oui
Composants de surveillance des comportements		
Modèle de détection de la surveillance des comportements (32 bits)	Oui	Oui
Pilote de surveillance des comportements (32 bits)	Oui	Oui
Service principal de surveillance des comportements (32 bits)	Oui	Oui
Modèle de détection de la surveillance des comportements (64 bits)	Oui	Oui
Pilote de surveillance des comportements (64 bits)	Oui	Oui
Service principal de surveillance des comportements (64 bits)	Oui	Oui
Modèle de configuration de la surveillance des comportements	Oui	Oui
Modèle de conformité aux stratégies	Oui	Oui
Digital Signature Pattern	Oui	Oui
Fichier de signatures de déclenchement du scan de la mémoire (32 bits)	Oui	Oui
Fichier de signatures de déclenchement du scan de la mémoire (64 bits)	Oui	Oui

Composant	Distribution	
	Agents de scan traditionnel	Agents Smart Scan
Service d'alerte de contact C&C		
Liste d'adresses IP C&C globale	Oui	Oui
Fichier de signatures de règle de pertinence	Oui	Oui
Solution contre l'exploitation du navigateur		
Fichier de signatures de prévention contre l'exploitation du navigateur	Oui	Oui
Fichier de signatures de l'analyseur de script	Oui	Oui

Rappels de mise à jour et conseils :

- Pour permettre au serveur de déployer les composants mis à jour sur les agents, activez la mise à jour automatique des agents. Pour obtenir des informations détaillées, consultez la section *Mises à jour automatiques des agents OfficeScan à la page 6-42*. Si la mise à jour automatique des agents est désactivée, le serveur télécharge les mises à jour mais ne les déploie pas sur les agents.
- Un serveur OfficeScan IPv6 pur ne peut pas distribuer de mises à jour directement à des agents IPv4 purs. De même, un serveur OfficeScan IPv4 pur ne peut pas distribuer de mises à jour directement à des agents IPv6 purs. Un serveur proxy à double pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre au serveur OfficeScan de distribuer une mise à jour aux agents.
- Trend Micro publie des fichiers de signatures régulièrement pour maintenir à jour la protection des agents. De nouveaux fichiers de mise à jour étant régulièrement mis à disposition, OfficeScan utilise un mécanisme appelé **duplication des composants** permettant une mise à jour plus rapide des fichiers de signatures. Voir *Duplication des composants du serveur OfficeScan à la page 6-23* pour obtenir plus d'informations.
- Si vous utilisez un serveur proxy pour vous connecter à Internet, utilisez les paramètres proxy corrects pour réussir le téléchargement des mises à jour.

- Sur le Tableau de bord de la console Web, ajoutez le widget **Mises à jour de l'agent** pour afficher les versions actuelles des composants et déterminer le nombre d'agents ayant des composants à jour et obsolètes.

Sources de mise à jour du serveur OfficeScan

Configurez le serveur Smart Protection Server pour qu'il télécharge Smart Scan Pattern à partir du serveur Trend Micro ActiveUpdate ou d'une autre source. Vous pouvez indiquer une autre source si le serveur OfficeScan est incapable d'accéder directement au serveur ActiveUpdate. Pour un exemple de scénario, voir *Mises à jour de serveur OfficeScan isolé à la page 6-26*.

Une fois les mises à jour disponibles téléchargées par le serveur, celui-ci peut automatiquement demander aux agents de mettre à jour leurs composants en fonction des paramètres spécifiés sous **Mises à jour** > **Agents** > **Mise à jour automatique**. Si la mise à jour des composants est critique, laissez au serveur le soin d'envoyer une notification aux agents en accédant à **Mises à jour** > **Agents** > **Mise à jour manuelle**.



Remarque

si vous ne spécifiez pas une programmation de déploiement ou des paramètres de mises à jour déclenchées par un événement dans **Mises à jour** > **Agents** > **Mise à jour automatique**, le serveur télécharge les mises à jour mais ne demande pas aux agents de procéder à la mise à jour.

Prise en charge d'IPv6 pour les mises à jour du serveur OfficeScan

Un serveur OfficeScan IPv6 pur ne peut effectuer directement de mises à jour à partir de sources de mise à jour IPv4 pures, telles que :

- Trend Micro ActiveUpdate Server
- Toute source de mise à jour personnalisée IPv4 pure

De même, un serveur OfficeScan IPv4 pur ne peut effectuer directement de mises à jour à partir de sources de mise à jour personnalisées IPv6 pures.

Un serveur proxy double-pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre au serveur de se connecter aux sources de mises à jour.

Proxy for OfficeScan Server Updates

Configurez les programmes du serveur hébergés sur l'ordinateur du serveur pour utiliser les paramètres proxy lors du téléchargement des mises à jour à partir du serveur Trend Micro ActiveUpdate. Les programmes du serveur incluent le serveur OfficeScan et le serveur Smart Protection Server intégré.

Configuration des paramètres proxy

Procédure

1. Accédez à **Administration** > **Paramètres** > **Proxy**.
2. Cliquez sur l'onglet **Proxy externe**.
3. Rendez-vous à la section **Mises à jour de l'ordinateur du serveur OfficeScan**.
4. Sélectionnez **Utiliser un serveur proxy pour les mises à jour de licence, de moteur ou de fichier de signatures**.
5. Indiquez le protocole de proxy, le nom ou l'adresse IPv4/IPv6 et le numéro de port du serveur proxy.
6. Si le serveur proxy nécessite une authentification, tapez le nom d'utilisateur et le mot de passe appropriés.
7. Cliquez sur **Enregistrer**.

Configuration de la source de mise à jour du serveur

Procédure

1. Accédez à **Mises à jour** > **Serveur** > **Source de mise à jour**.

2. Sélectionnez l'emplacement depuis lequel vous souhaitez télécharger les mises à jour de composants.

   Si vous choisissez le serveur ActiveUpdate, assurez-vous qu'il dispose d'une connexion Internet et, si vous utilisez un serveur proxy, testez si la connexion Internet peut être établie en utilisant les paramètres du proxy. Pour obtenir des informations détaillées, voir *Proxy for OfficeScan Server Updates à la page 6-22*.

   Si vous choisissez une source de mise à jour personnalisée, définissez l'environnement approprié et mettez à jour les ressources de cette source de mise à jour. Assurez-vous également qu'il existe une connexion opérationnelle entre le serveur et cette source de mise à jour. Si vous avez besoin d'aide pour définir une source de mise à jour, contactez votre service d'assistance.

   Remarque

   Le serveur OfficeScan utilise la duplication de composants lors du téléchargement des composants depuis la source de mise à jour. Voir *Duplication des composants du serveur OfficeScan à la page 6-23* pour obtenir des informations détaillées.

3. Cliquez sur **Enregistrer**.

Duplication des composants du serveur OfficeScan

Lorsque la dernière version d'un fichier de signatures complet est disponible au téléchargement sur le serveur Trend Micro ActiveUpdate server, 14 « fichiers de signatures incrémentiels » deviennent également disponibles. Les fichiers de signatures incrémentiels constituent des versions moins volumineuses que le fichier de signatures complet et correspondent à la différence entre la version la plus récente et la version précédente du fichier de signatures complet. Par exemple, si la version la plus récente est la version 175, le fichier de signatures incrémentiel v_173.175 contient les signatures de la version 175 absentes de la version 173 (la version 173 est la version précédente du fichier de signatures complet, puisque les numéros des fichiers de signatures sont déterminés par incrémentation de 2). Le fichier de signatures incrémentiel v_171.175 contient les signatures de la version 175 absentes de la version 171.

Pour réduire le trafic réseau généré lors du téléchargement du fichier de signatures le plus récent, OfficeScan effectue une duplication des composants, une méthode de mise

à jour par laquelle le serveur OfficeScan ou l'agent de mise à jour télécharge uniquement les fichiers de signatures incrémentiels. Voir *Duplication des composants d'un agent de mise à jour à la page 6-66* pour plus d'informations sur la manière dont les agents de mise à jour dupliquent les composants.

La duplication des composants s'applique aux composants suivant :

- Fichier de signatures de virus
- Smart Scan Agent Pattern
- Modèle de nettoyage de virus
- Signatures d'exceptions IntelliTrap
- Signatures de spywares
- Signatures de surveillance active des spywares

Scénario de duplication des composants

Pour comprendre le processus de duplication des composants pour le serveur, reportez-vous au scénario suivant :

TABLEAU 6-5. Scénario de duplication des composants du serveur

Fichiers de signatures complets sur le serveur OfficeScan	Version actuelle : 171					
	Autres versions disponibles :					
	169	167	165	161	159	
Dernière version sur le serveur ActiveUpdate	173.175	171.175	169.175	167.175	165.175	163.175
	161.175	159.175	157.175	155.175	153.175	151.175
	149.175	147.175				

1. Le serveur OfficeScan compare la version actuelle de son fichier de signatures complet avec la dernière version disponible sur le serveur ActiveUpdate. Si la différence entre les deux versions est inférieure ou égale à 14, le serveur ne télécharge que le fichier de signatures incrémentiel qui correspond à la différence entre les deux versions.



Remarque

si la différence est supérieure à 14, le serveur télécharge automatiquement la version complète du fichier de signatures et 14 fichiers de signatures incrémentiels.

Voici un exemple :

- La différence entre les versions 171 et 175 est de 2. En d'autres termes, le serveur ne dispose pas des versions 173 et 175.
- Le serveur télécharge les fichiers de signatures incrémentiels 171.175. Le fichier de signatures incrémentiel correspond à la différence entre les versions 171 et 175.

2. Le serveur fusionne le fichier de signatures incrémentiel avec son fichier de signatures complet actuel pour générer le fichier de signatures complet le plus récent.

   Voici un exemple :

   - Sur le serveur, OfficeScan fusionne la version 171 avec le fichier de signatures incrémentiel 171.175 pour générer la version 175.
   - Le serveur dispose d'un fichier de signatures incrémentiel (171.175) et du fichier de signatures complet le plus récent (version 175).

3. Le serveur génère des fichiers de signatures incrémentiels en fonction des autres fichiers de signatures complets disponibles sur le serveur. Si le serveur ne génère pas ces fichiers de signatures incrémentiels, les agents qui n'ont pas téléchargé les fichiers de signatures incrémentiels précédents procèdent automatiquement au téléchargement du fichier de signatures complet, ce qui entraîne une augmentation du trafic réseau.

   Voici un exemple :

   - Le serveur dispose des versions 169, 167, 165, 163, 161 et 159. Il peut donc générer les fichiers de signatures incrémentiels suivants :

     169.175, 167.175, 165.175, 163.175, 161.175, 159.175

   - Dans la mesure où le serveur dispose déjà du fichier de signatures incrémentiel 171.175, il n'a pas besoin d'utiliser la version 171.

- Le serveur dispose maintenant de 7 fichiers de signatures incrémentiels :

  171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175

- Le serveur conserve les 7 derniers fichiers de signatures complets (versions 175, 171, 169, 167, 165, 163, 161). Il supprime toute version antérieure (version 159).

4. Le serveur compare ses fichiers de signatures incrémentiels actuels avec ceux disponibles sur le serveur ActiveUpdate. Le serveur télécharge les fichiers de signatures incrémentiels dont il ne dispose pas.

   Voici un exemple :

   - Le serveur ActiveUpdate dispose de 14 fichiers de signatures incrémentiels :

     173.175, 171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175, 157.175, 155.175, 153.175, 151.175, 149.175, 147.175

   - Le serveur OfficeScan dispose de 7 fichiers de signatures incrémentiels :

     171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175

   - Le serveur OfficeScan procède au téléchargement de 7 fichiers de signatures incrémentiels supplémentaires :

     173.175, 157.175, 155.175, 153.175, 151.175, 149.175, 147.175

   - Le serveur dispose maintenant de tous les fichiers de signatures incrémentiels disponibles sur le serveur ActiveUpdate.

5. Le fichier de signatures complet et les 14 fichiers de signatures incrémentiels sont mis à la disposition des agents.

Mises à jour de serveur OfficeScan isolé

Si le serveur OfficeScan appartient à un réseau qui est totalement isolé de l'ensemble des sources externes, vous pouvez maintenir les composants du serveur à jour en autorisant ce dernier à se mettre à jour depuis une source interne contenant les derniers composants.

Cette rubrique explique les tâches que vous devrez réaliser afin de mettre à jour un serveur OfficeScan isolé.

Mise à jour d'un serveur OfficeScan isolé

Cette procédure est fournie à titre informatif. Si vous êtes en mesure de réaliser toutes les tâches de cette procédure, veuillez contacter votre fournisseur d'accès pour obtenir des informations détaillées concernant chaque tâche de la procédure.

Procédure

1. Identifiez la source de mise à jour, par exemple, Trend Micro Control Manager ou un ordinateur hôte choisi aléatoirement. La source de mise à jour doit comprendre les éléments suivants :

    - Une connexion Internet fiable, pour qu'elle puisse télécharger les derniers composants à partir du serveur Trend Micro ActiveUpdate. Sans connexion Internet, la seule façon pour la source de mise à jour d'obtenir les derniers composants est que vous récupériez les composants vous-même à partir de Trend Micro et que vous les copiez dans la source de mise à jour.

    - Une connexion opérationnelle au serveur OfficeScan. Configurez les paramètres proxy si un serveur proxy se trouve entre le serveur OfficeScan et la source de mise à jour. Pour obtenir des informations détaillées, voir *Proxy for OfficeScan Server Updates à la page 6-22*.

    - Suffisamment d'espace disque pour les composants téléchargés.

2. Faites pointer le serveur OfficeScan vers la nouvelle source de mise à jour. Pour obtenir des informations détaillées, voir *Sources de mise à jour du serveur OfficeScan à la page 6-21*.

3. Identifiez les composants déployés sur les agents par le serveur. Voir *Mises à jour des agents OfficeScan à la page 6-31* pour obtenir la liste des composants déployables.



Conseil

L'un des moyens permettant de déterminer si un composant est en cours de déploiement sur des agents consiste à accéder à l'écran **Résumé des mises à jour** de la console Web (**Mises à jour** > **Résumé**). Dans cet écran, le taux de mise à jour d'un composant en cours de déploiement est toujours supérieur à 0 %.

4. Déterminez à quelle fréquence télécharger les composants. Les fichiers de signatures sont régulièrement mis à jour (quotidiennement dans certains cas), il est donc recommandé de les mettre à jour régulièrement. Pour les moteurs de scan et les pilotes, vous pouvez demander à votre service d'assistance de vous avertir en cas de mise à jour critique.

5. Concernant la source de mise à jour :

   a. Connectez-vous au serveur ActiveUpdate. L'URL du serveur dépend de votre version d'OfficeScan.

   b. Téléchargez les éléments suivants :

      - Le fichier `server.ini`. Ce fichier contient des informations sur les composants les plus récents.

      - Les composants que vous avez identifiés à l'étape 3.

   c. Enregistrez les éléments enregistrés dans un répertoire de la source de mise à jour.

6. Exécutez une mise à jour manuelle du serveur OfficeScan. Pour obtenir des informations détaillées, voir *Mise à jour manuelle du serveur OfficeScan à la page 6-29*.

7. Répétez les étapes 5 et 6 chaque fois que vous devez mettre à jour des composants.

Méthodes de mise à jour du serveur OfficeScan

Mettez à jour les composants du serveur OfficeScan manuellement ou en configurant un programme de mise à jour.

Pour permettre au serveur de déployer les composants mis à jour sur les agents, activez la mise à jour automatique des agents. Pour obtenir des informations détaillées, voir *Mises à jour automatiques des agents OfficeScan à la page 6-42*. Si la mise à jour automatique

des agents est désactivée, le serveur télécharge les mises à jour mais ne les déploie pas sur les agents.

Les méthodes de mise à jour comprennent :

- **Mise à jour manuelle du serveur** : Lorsqu'une mise à jour est capitale, effectuez une mise à jour manuelle afin que le serveur puisse obtenir les mises à jour immédiatement. Voir *Mise à jour manuelle du serveur OfficeScan à la page 6-29* pour obtenir des informations détaillées.
- **Mise à jour programmée du serveur** : Le serveur OfficeScan se connecte à la source de mise à jour au jour et à l'heure programmés pour obtenir les composants les plus récents. Voir *Programmation de mises à jour du serveur OfficeScan à la page 6-29* pour obtenir des informations détaillées.

Mise à jour manuelle du serveur OfficeScan

Mettez à jour manuellement les composants sur le serveur OfficeScan après l'installation ou la mise à niveau du serveur OfficeScan et en cas d'épidémie.

Procédure

1. Commencez une mise à jour manuelle par :
   - Accédez à **Mises à jour** > **Serveur** > **Mise à jour manuelle**.
   - Cliquez sur **Mise à jour immédiate du serveur** dans le menu principal de la console Web.
2. Sélectionnez les composants à mettre à jour.
3. Cliquez sur **Mettre à jour**.

   Le serveur télécharge les composants mis à jour.

Programmation de mises à jour du serveur OfficeScan

Configurez le serveur OfficeScan afin de vérifier régulièrement sa source de mise à jour et de télécharger automatiquement les mises à jour disponibles. Comme les agents

reçoivent normalement des mises à jour du serveur, l'utilisation de la mise à jour programmée est un moyen simple et efficace de garantir que la protection contre les risques de sécurité est mise à jour en permanence.

Procédure

1. Accédez à **Mises à jour** > **Serveur** > **Mise à jour programmée**.
2. Sélectionnez **Activer la mise à jour programmée du serveur OfficeScan**.
3. Sélectionnez les composants à mettre à jour.
4. Programmez les mises à jour.

   Pour des mises à jour quotidiennes, hebdomadaires et mensuelles, la période correspond au nombre d'heures pendant lesquelles OfficeScan exécute la mise à jour. OfficeScan procède à la mise à jour à tout moment pendant cette période.
5. Cliquez sur **Enregistrer**.

Journaux de mise à jour du serveur OfficeScan

Consultez les journaux de mise à jour du serveur pour déterminer s'il existe des problèmes de mise à jour de certains composants. Les journaux incluent les mises à jour de composants pour le serveur OfficeScan.

Pour éviter que les journaux n'occupent trop d'espace sur votre disque dur, vous pouvez les supprimer manuellement ou configurer leur suppression programmée. Voir *Gestion du journal à la page 13-36* pour obtenir des informations complémentaires sur la gestion des journaux.

Affichage des journaux de mise à jour

Procédure

1. Accédez à **Journaux** > **Mise à jour du serveur**.
2. Consultez la colonne **Résultat** pour vérifiez si des composants n'ont pas été mis à jour.

3. Pour sauvegarder les journaux dans un fichier CSV (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Mises à jour du serveur Smart Protection Server intégré

L'Integrated Smart Protection Server intégré Smart Protection Server télécharge deux composants, appelés le Smart Scan Pattern et la Liste de blocage de sites Web. Pour obtenir des informations sur ces composants et leur méthode de mise à jour, consultez la rubrique *Gestion du serveur Smart Protection Server intégré à la page 4-20*.

Mises à jour des agents OfficeScan

Pour garantir le maintien de la protection des agents contre les risques de sécurité les plus récents, procédez à une mise à jour régulière des composants des agents.

Avant de mettre à jour les agents, vérifiez que leur source de mise à jour (un serveur OfficeScan ou une source de mise à jour personnalisée) possède les composants les plus récents. Voir *Mises à jour du serveur OfficeScan à la page 6-17* pour obtenir des informations sur la méthode de mise à jour du serveur OfficeScan.

Le tableau suivant répertorie tous les composants que les sources de mise à jour déploient sur les agents et les composants utilisés selon la méthode de scan applicable.

TABLEAU 6-6. Composants OfficeScan déployés sur les agents

COMPOSANT	DISTRIBUTION	
	AGENTS DE SCAN TRADITIONNEL	AGENTS SMART SCAN
Antivirus		
Smart Scan Agent Pattern	Non	Oui

Composant	Distribution	
	Agents de scan traditionnel	Agents Smart Scan
Fichier de signatures de virus	Oui	Non
Signatures IntelliTrap	Oui	Oui
Signatures d'exceptions IntelliTrap	Oui	Oui
Moteur de scan antivirus (32 bits)	Oui	Oui
Moteur de scan antivirus (64 bits)	Oui	Oui
Fichier de signatures d'inspection de la mémoire	Oui	Oui
Anti-spyware		
Fichier de signatures des spywares/ graywares	Oui	Oui
Signatures de surveillance active des spywares	Oui	Non
Moteur de scan anti-spywares/ graywares (32 bits)	Oui	Oui
Moteur de scan anti-spywares/ graywares (64 bits)	Oui	Oui
Damage Cleanup Services		
Modèle Damage Cleanup	Oui	Oui
Moteur Damage Cleanup (32 bits)	Oui	Oui
Moteur Damage Cleanup (64 bits)	Oui	Oui
Early Boot Clean Driver (32 bits)	Oui	Oui
Early Boot Clean Driver (64 bits)	Oui	Oui
Services de réputation de sites Web		

Composant	Distribution	
	Agents de scan traditionnel	Agents Smart Scan
Moteur de filtre URL	Oui	Oui
Pare-feu		
Fichier de signatures du pare-feu	Oui	Oui
Pilote du pare-feu (32 bits)	Oui	Oui
Pilote du pare-feu (64 bits)	Oui	Oui
Composants de surveillance des comportements		
Modèle de détection de la surveillance des comportements (32 bits)	Oui	Oui
Pilote principal de surveillance des comportements (32 bits)	Oui	Oui
Service principal de surveillance des comportements (32 bits)	Oui	Oui
Modèle de détection de la surveillance des comportements (64 bits)	Oui	Oui
Pilote principal de surveillance des comportements (64 bits)	Oui	Oui
Service principal de surveillance des comportements (64 bits)	Oui	Oui
Modèle de configuration de la surveillance des comportements	Oui	Oui
Modèle de conformité aux stratégies	Oui	Oui
Digital Signature Pattern	Oui	Oui

COMPOSANT	DISTRIBUTION	
	AGENTS DE SCAN TRADITIONNEL	AGENTS SMART SCAN
Fichier de signatures de déclenchement du scan de la mémoire (32 bits)	Oui	Oui
Fichier de signatures de déclenchement du scan de la mémoire (64 bits)	Oui	Oui
Connexions suspectes		
Liste d'adresses IP C&C globale	Oui	Oui
Fichier de signatures de règle de pertinence	Oui	Oui
Exploitations du navigateur		
Fichier de signatures de prévention contre l'exploitation du navigateur	Oui	Oui
Fichier de signatures de l'analyseur de script	Oui	Oui

Sources de mise à jour des agents OfficeScan

Les agents peuvent obtenir des mises à jour depuis la source de mise à jour standard (serveur OfficeScan) ou des composants spécifiques depuis des sources de mises à jour personnalisées, telles que le serveur ActiveUpdate de Trend Micro. Pour obtenir des informations détaillées, voir *Source de mise à jour standard pour les agents OfficeScan à la page 6-35* et *Sources de mise à jour personnalisées pour les agents OfficeScan à la page 6-36*.

Prise en charge d'IPv6 pour les mises à jour des agents OfficeScan

Un agent IPv6 pur ne peut pas effectuer de mises à jour à partir de sources de mise à jour IPv4 pures, telles que :

- un serveur OfficeScan IPv4 pur
- un agent de mise à jour IPv4 pur
- Toute source de mise à jour personnalisée IPv4 pure
- Trend Micro ActiveUpdate Server

De même, un agent IPv4 pur ne peut pas effectuer de mises à jour à partir de sources de mise à jour IPv6 pures, telles qu'un serveur OfficeScan ou un agent de mise à jour IPv6 pur.

Un serveur proxy à double pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre aux agents de se connecter aux sources de mises à jour.

Source de mise à jour standard pour les agents OfficeScan

Le serveur OfficeScan est la source de mise à jour standard pour les agents.

Si le serveur OfficeScan est injoignable, les agents ne disposeront pas de source de sauvegarde et seront par conséquent obsolètes. Pour mettre à jour les agents qui ne peuvent pas se connecter au serveur OfficeScan, Trend Micro recommande d'utiliser Agent Packager. Utilisez cet outil pour créer un package contenant les composants les plus récents disponibles sur le serveur, puis exécutez ce package sur les agents.



Remarque

L'adresse IP de l'agent (IPv4 ou IPv6) détermine si la connexion au serveur OfficeScan peut être établie. Pour plus d'informations sur la prise en charge d'IPv6 pour les mises à jour des agents, voir *Prise en charge d'IPv6 pour les mises à jour des agents OfficeScan à la page 6-34*.

Configuration de la source de mise à jour standard des agents OfficeScan

Procédure

1. Accédez à **Mises à jour** > **Agents** > **Source de mise à jour**.
2. Sélectionnez **Source de mise à jour standard (mise à jour depuis le serveur OfficeScan)**.

3. Cliquez sur **Notifier tous les agents**.

Processus de mise à jour des agents OfficeScan



Remarque

Cette rubrique explique le processus de mise à jour des agents OfficeScan. Le processus de mise à jour des agents de mise à jour est traité dans la section *Source de mise à jour standard pour les agents OfficeScan à la page 6-35*.

Si vous configurez les agents OfficeScan pour la mise à jour directe à partir du serveur OfficeScan, le processus de mise à jour s'effectue de la façon suivante :

1. L'agent OfficeScan obtient les mises à jour à partir du serveur OfficeScan.
2. Si la mise à jour à partir du serveur OfficeScan est impossible, l'agent OfficeScan essaie de se connecter directement au serveur ActiveUpdate de Trend Micro si l'option **Les agents OfficeScan téléchargent des mises à jour depuis le serveur ActiveUpdate de Trend Micro** est activée sous **Agents** > **Gestion des agents**, puis sous **Paramètres** > **Privilèges et autres paramètres** > **Autres paramètres (onglet)** > **Paramètres de mise à jour**.



Remarque

Seuls les composants peuvent être mis à jour depuis le serveur ActiveUpdate. Les paramètres de domaine, les programmes et les correctifs de type hot fix ne peuvent être téléchargés qu'à partir du serveur OfficeScan ou des agents de mise à jour. Vous pouvez accélérer le processus de mise à jour en configurant les agents OfficeScan pour qu'ils téléchargent uniquement des fichiers de signature à partir du serveur ActiveUpdate. Pour plus d'informations, voir *Serveur ActiveUpdate en tant que source de mise à jour des agents OfficeScan à la page 6-41*.

Sources de mise à jour personnalisées pour les agents OfficeScan

Outre le serveur OfficeScan, les agents OfficeScan peuvent être mis à jour depuis des sources de mise à jour personnalisées. Les sources de mise à jour personnalisées

contribuent à la réduction du trafic de mise à jour des agents OfficeScan dirigé vers le serveur OfficeScan et permettent aux agents OfficeScan ne pouvant pas se connecter au serveur OfficeScan d'obtenir des mises à jour rapides. Spécifiez les sources de mise à jour personnalisées dans la Liste de sources de mise à jour personnalisées, qui peut accueillir jusqu'à 1024 sources de mise à jour.



Conseil

Trend Micro recommande de définir certains agents OfficeScan en tant qu'agents de mise à jour et de les ajouter à la liste.

Configuration des sources de mise à jour personnalisées pour les agents OfficeScan

Procédure

1. Accédez à **Mises à jour** > **Agents** > **Source de mise à jour**.
2. Sélectionnez **Sources de mise à jour personnalisées** et cliquez sur **Ajouter**.
3. Dans l'écran qui s'affiche, indiquez les adresses IP des agents. Vous pouvez entrer une plage d'adresses IPv4 et/ou un préfixe IPv6 et sa longueur.
4. Spécifiez la source de mise à jour. Vous pouvez sélectionner un agent de mise à jour si un tel agent a été affecté ou saisir l'URL d'une source spécifique.



Remarque

Assurez-vous que les agents OfficeScan peuvent se connecter à la source de mise à jour en utilisant leurs adresses IP. Par exemple, si vous avez indiqué une plage d'adresses IPv4, la source de mise à jour doit avoir une adresse IPv4. Si vous avez indiqué un préfixe IPv6 et une longueur, la source de mise à jour doit avoir une adresse IPv6. Pour plus d'informations sur la prise en charge d'IPv6 pour les mises à jour des agents, voir *Sources de mise à jour des agents OfficeScan à la page 6-34*.

5. Cliquez sur **Enregistrer**.
6. Exécutez des tâches diverses présentées à l'écran.

a. Sélectionnez l'un des paramètres suivants. Pour plus de détails sur la gestion de ces paramètres, reportez-vous à *Processus de mise à jour des agents OfficeScan à la page 6-36*.

   - **Les agents de mise à jour effectuent la mise à jour des composants, des paramètres du domaine, des programmes des agents et des correctifs de type hot fix, uniquement à partir du serveur OfficeScan**
   - Les agents OfficeScan mettent à jour les éléments suivants à partir du serveur OfficeScan si toutes les sources personnalisées sont indisponibles ou introuvables :
     - **Composants**
     - **Paramètres de domaine**
     - **Programmes et correctifs de type hot fix des agents OfficeScan**

b. Si vous avez indiqué au moins un agent de mise à jour en tant que source, cliquez sur **Rapport d'analyse de l'agent de mise à jour** pour générer un rapport mettant en évidence l'état de la mise à jour des agents. Pour plus de détails sur ce rapport, voir *Rapport d'analyse de l'agent de mise à jour à la page 6-68*.

c. Modifiez une source de mise à jour en cliquant sur le lien Plage d'adresses IP. Modifiez les paramètres dans l'écran qui s'affiche puis cliquez sur **Enregistrer**.

d. Supprimez une source de mise à jour depuis la liste en cochant la case correspondante et en cliquant sur **Supprimer**.

e. Pour déplacer une source de mise à jour, cliquez sur la flèche haut ou bas. Vous ne pouvez déplacer qu'une source à la fois.

7. Cliquez sur **Notifier tous les agents**.

Processus de mise à jour des agents OfficeScan



Remarque

Cette rubrique explique le processus de mise à jour des agents OfficeScan. Le processus de mise à jour des agents de mise à jour est traité dans la section *Sources de mises à jour personnalisées pour les agents de mises à jour à la page 6-64*.

Après avoir défini et enregistré la liste des sources de mise à jour personnalisées, le processus de mise à jour s'effectue de la façon suivante :

1. L'agent OfficeScan est mis à jour à partir de la première source de la liste.
2. Si la mise à jour est impossible à partir de la première source, l'agent OfficeScan essaie avec la seconde source, et ainsi de suite.
3. Si la mise à jour n'est possible à partir d'aucune des sources, l'agent OfficeScan vérifie les paramètres suivants sur l'écran **Source de mise à jour** :

Tableau 6-7. Paramètres supplémentaires de sources de mise à jour personnalisées

Paramètre	Description
Les agents de mise à jour effectuent la mise à jour des composants, des paramètres du domaine, des programmes des agents et des correctifs de type hot fix, uniquement à partir du serveur OfficeScan	Si ce paramètre est actif, les agents de mise à jour s'exécutent directement à partir du serveur OfficeScan et ignorent l'option Liste des sources de mise à jour personnalisées. Si ce paramètre est désactivé, les agents de mise à jour appliquent les paramètres de source de mise à jour personnalisée configurés pour des agents normaux.
Les agents OfficeScan mettent à jour les éléments suivants à partir du serveur OfficeScan si toutes les sources personnalisées sont indisponibles ou introuvables :	

Paramètre	Description
Composants	Si ce paramètre est activé, l'agent procède à la mise à jour des composants à partir du serveur OfficeScan. S'il est désactivé, l'agent essaie ensuite de se connecter directement au serveur ActiveUpdate de Trend Micro si l'une des conditions suivantes est vérifiée : • Sous **Agents** > **Gestion des agents**, puis sous **Paramètres** > **Privilèges et autres paramètres** > **Autres paramètres (onglet)** > **Paramètres de mise à jour**, l'option **Les agents OfficeScan téléchargent des mises à jour depuis le serveur ActiveUpdate de Trend Micro** est activée. • Le serveur ActiveUpdate n'est pas inclus dans la liste de sources de mise à jour personnalisées. **Remarque** Seuls les composants peuvent être mis à jour depuis le serveur ActiveUpdate. Les paramètres de domaine, les programmes et les correctifs de type hot fix ne peuvent être téléchargés qu'à partir du serveur OfficeScan ou des agents de mise à jour. Vous pouvez accélérer le processus de mise à jour en configurant les agents pour qu'ils téléchargent uniquement des fichiers de signature à partir du serveur ActiveUpdate. Pour plus d'informations, voir *Serveur ActiveUpdate en tant que source de mise à jour des agents OfficeScan à la page 6-41*.
Paramètres de domaine	Si ce paramètre est activé, l'agent met à jour les paramètres au niveau du domaine à partir du serveur OfficeScan.
Programmes et correctifs de type hot fix des agents OfficeScan	Si ce paramètre est activé, l'agent met à jour les programmes et les correctifs de type hot fix à partir du serveur OfficeScan.

4. S'il ne peut pas obtenir les mises à jour à partir des sources possibles, l'agent abandonne le processus de mise à jour.

Serveur ActiveUpdate en tant que source de mise à jour des agents OfficeScan

Lorsque les agents OfficeScan téléchargent des mises à jour directement depuis le serveur ActiveUpdate de Trend Micro, vous pouvez restreindre le téléchargement aux fichiers de signatures afin de réduire la bande passante consommée et accélérer le processus.

Les moteurs de scan et autres composants ne sont pas mis à jour aussi régulièrement que des fichiers de signatures, ce qui justifie là aussi le fait de restreindre le téléchargement aux fichiers de signatures uniquement.

Un agent IPv6 pur ne peut pas directement effectuer de mise à jour à partir du serveur ActiveUpdate de Trend Micro. Un serveur proxy à double pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre aux agents OfficeScan de se connecter au serveur ActiveUpdate.

Limitation des téléchargements à partir du serveur ActiveUpdate

---

Procédure

1. Accédez à **Agents** > **Paramètres généraux de l'agent**.
2. Accédez à la section **Mises à jour**.
3. Sélectionnez **Télécharger uniquement les fichiers de signatures du serveur ActiveUpdate lors de l'exécution des mises à jour**.

Méthodes de mise à jour des agents OfficeScan

Les agents OfficeScan qui mettent à jour des composants à partir du serveur OfficeScan ou d'une source de mise à jour personnalisée peuvent utiliser les méthodes de mise à jour suivantes :

- **Mises à jour automatiques** : la mise à jour des agents s'exécute automatiquement lorsque certains événements se produisent ou en fonction d'une programmation. Pour obtenir des informations détaillées, voir *Mises à jour automatiques des agents OfficeScan à la page 6-42*.

- **Mises à jour manuelles** : Lorsqu'une mise à jour est capitale, effectuez une mise à jour manuelle pour demander immédiatement aux agents d'effectuer la mise à jour des composants. Pour obtenir des informations détaillées, voir *Mises à jour manuelles des agents OfficeScan à la page 6-49*.
- **Mises à jour en fonction des privilèges** : Les utilisateurs disposant de privilèges de mise à jour ont davantage de contrôle sur la manière dont l'agent OfficeScan présent sur leur ordinateur est mis à jour. Pour obtenir des informations détaillées, voir *Configuration des privilèges de mise à jour et d'autres paramètres à la page 6-51*.

Mises à jour automatiques des agents OfficeScan

La mise à jour automatique vous évite d'avoir à demander à tous les agents d'effectuer une mise à jour et supprime tout risque de présence de composants obsolètes sur des ordinateurs des agents.

Outre ces composants, les agents OfficeScan reçoivent également des fichiers de configuration mis à jour au cours de la mise à jour automatique. Les agents ont besoin des fichiers de configuration pour appliquer les nouveaux paramètres. À chaque fois que vous modifiez les paramètres d'OfficeScan via la console Web, les fichiers de configuration sont modifiés. Pour spécifier la fréquence à laquelle les fichiers de configuration sont appliqués aux agents, reportez-vous à l'étape 3 *Configuration des mises à jour automatiques des agents OfficeScan à la page 6-44*.



Remarque

Vous pouvez configurer les agents pour qu'ils utilisent des paramètres proxy lors de la mise à jour automatique. Voir *Proxy pour les mises à jour des composants des agents OfficeScan à la page 6-54* pour obtenir des informations détaillées.

Il existe deux types de mise à jour automatique :

- *Mises à jour déclenchées par un événement à la page 6-42*
- *Mises à jour programmées à la page 6-44*

Mises à jour déclenchées par un événement

Le serveur peut demander aux agents en ligne de mettre à jour les composants une fois le téléchargement des composants les plus récents effectué et informer les agents hors

ligne lorsqu'ils redémarrent et se connectent au serveur. Vous pouvez également exécuter un scan immédiat (scan manuel) sur les ordinateurs des agents OfficeScan après la mise à jour.

Tableau 6-8. Options de mise à jour déclenchée par un événement

Option	Description
Lancer la mise à jour des composants sur les agents immédiatement après le téléchargement d'un nouveau composant par le serveur OfficeScan	Le serveur demande aux agents d'effectuer la mise à jour dès qu'il a lui-même terminé une mise à jour. Les agents mis à jour fréquemment ne doivent télécharger que des fichiers de signatures incrémentiels, ce qui réduit le temps nécessaire à la mise à jour (voir *Duplication des composants du serveur OfficeScan à la page 6-23* pour plus d'informations sur les fichiers de signatures incrémentiels). Toutefois, de fréquentes mises à jour peuvent nuire aux performances du serveur, en particulier si un grand nombre d'agents effectuent une mise à jour en même temps. Si vous souhaitez mettre à jour des agents qui se trouvent en mode itinérant, sélectionnez l'option Inclure le ou les agents itinérants et hors ligne. Voir *Privilège des agents OfficeScan itinérants à la page 14-21* pour plus d'informations sur le mode itinérant.
Permettre aux agents de lancer une mise à jour des composants lorsqu'ils redémarrent et se connectent au serveur OfficeScan (les agents itinérants sont exclus)	Un agent ayant manqué une mise à jour télécharge immédiatement les composants lorsqu'il établit une connexion avec le serveur. Il se peut qu'un agent manque une mise à jour s'il est hors ligne ou si le endpoint sur lequel il est installé ne fonctionne pas.
Exécuter un scan immédiat après la mise à jour (les agents itinérants sont exclus)	Le serveur demande aux agents d'effectuer un scan après une mise à jour déclenchée par un événement. Vous pouvez envisager d'activer cette option si une mise à jour particulière est une réponse à un risque de sécurité qui s'est déjà répandu sur le réseau.



Remarque

si le serveur OfficeScan ne parvient pas à envoyer une notification de mise à jour aux agents une fois le téléchargement des composants effectué, il renvoie automatiquement la notification passé un délai de 15 minutes. Le serveur envoie au maximum cinq notifications de mise à jour dans l'attente de la réponse des agents. Si la cinquième tentative est toujours infructueuse, le serveur arrête l'envoi des notifications. Si vous sélectionnez l'option de mise à jour des composants lorsque les agents redémarrent et se connectent au serveur, la mise à jour des composants ne sera pas interrompue.

Mises à jour programmées

L'exécution de mises à jour programmées est un privilège. Vous devez d'abord sélectionner les agents OfficeScan qui disposeront de ce privilège, puis ces agents OfficeScan exécuteront les mises à jour selon la programmation.



Remarque

Pour utiliser la mise à jour programmée avec le mécanisme de traduction d'adresse réseau (Network Address Translation), voir *Configuration des mises à jour programmées des agents OfficeScan avec NAT à la page 6-46*.

Configuration des mises à jour automatiques des agents OfficeScan

Procédure

1. Accédez à **Mises à jour** > **Agents** > **Mise à jour automatique**.
2. Sélectionnez les événements que vous souhaitez associer à la fonction **Mise à jour déclenchée par un événement** :
   - **Lancer la mise à jour des composants sur les agents immédiatement après le téléchargement d'un nouveau composant par le serveur OfficeScan**
     - **Inclure le ou les agents itinérants et hors ligne**

- **Permettre aux agents de lancer une mise à jour des composants lorsqu'ils redémarrent et se connectent au serveur OfficeScan (les agents itinérants sont exclus)**
- **Exécuter un scan immédiat après la mise à jour (les agents itinérants sont exclus)**

Pour plus de détails sur les options disponibles, voir *Mises à jour déclenchées par un événement à la page 6-42*.

3. Configurez la programmation pour la fonction **Mise à jour déclenché par un événement**.

- **Minute(s)** ou **Heure(s)**

  L'option **Mettre à jour les configurations des agents une seule fois par jour** est disponible lors de la programmation d'une mise à jour à intervalles d'une heure ou d'un certain nombre de minutes. Le fichier de configuration contient tous les paramètres des agents OfficeScan configurés à l'aide de la console Web.

  Conseil

  Trend Micro met à jour fréquemment les composants ; cependant, les paramètres de configuration d'OfficeScan changent probablement moins fréquemment. La mise à jour des fichiers de configuration avec les composants nécessite plus de bande passante et augmente le temps nécessaire à OfficeScan pour terminer la mise à jour. C'est la raison pour laquelle Trend Micro recommande de mettre à jour les configurations des agents OfficeScan une seule fois par jour.

- **Quotidienne** ou **Hebdomadaire**

  Indiquez l'heure de la mise à jour et la durée pendant laquelle le serveur OfficeScan demande aux agents de mettre à jour les composants.



Conseil

Ce paramètre permet d'éviter que tous les agents en ligne se connectent simultanément au serveur à l'heure spécifiée, réduisant de manière significative le trafic sur le serveur. Par exemple, si l'heure de début a été définie sur 12h00 et que la durée est de 2 heures, OfficeScan demande de façon aléatoire à tous les agents en ligne de mettre à jour les composants entre 12h00 et 14h00.



Remarque

Une fois la programmation de mise à jour configurée, activez cette programmation sur les agents sélectionnés. Pour plus d'informations sur l'activation des mises à jour programmées, voir l'étape 4 de la section *Configuration des privilèges de mise à jour et d'autres paramètres à la page 6-51*.

4. Cliquez sur **Enregistrer**.

   OfficeScan ne peut pas notifier immédiatement les agents hors ligne. Sélectionnez **Permettre aux agents de lancer une mise à jour des composants lorsqu'ils redémarrent et se connectent au serveur OfficeScan (les agents itinérants sont exclus)** pour mettre à jour les agents hors ligne qui sont à nouveau en ligne après l'expiration de la durée configurée. Les agents hors ligne sur lesquels ce paramètre n'est pas activé mettent à jour les composants lors de la mise à jour programmée suivante ou lors d'une mise à jour manuelle.

Configuration des mises à jour programmées des agents OfficeScan avec NAT

Les problèmes suivants peuvent se poser si le réseau local utilise NAT :

- Les agents OfficeScan apparaissent hors ligne sur la console Web.
- Le serveur OfficeScan n'est pas en mesure d'avertir les agents des mises à jour et des modifications de la configuration.

Contournez ces problèmes en déployant sur l'agent OfficeScan les composants et fichiers de configuration mis à jour issus du serveur OfficeScan à l'aide d'une mise à jour programmée, comme décrit ci-dessous.

Procédure

- Avant d'installer l'agent OfficeScan sur les ordinateurs des agents :

  a. Configurez la programmation de mise à jour des agents dans la section **Mise à jour programmée** de **Mises à jour** > **Agents** > **Mise à jour automatique**.

  b. Pour accorder aux agents le privilège d'activer la mise à jour programmée, accédez à **Agents** > **Gestion des agents**, puis cliquez sur **Paramètres** > **Privilèges et autres paramètres** > **Privilèges (onglet)** > **Privilèges de mise à jour des composants**.

- Si les agents OfficeScan existent déjà sur les ordinateurs des agents :

  a. Pour accorder aux agents le privilège d'exécuter l'action « Mettre à jour », accédez à **Agents** > **Gestion des agents**, puis cliquez sur **Paramètres** > **Privilèges et autres paramètres** > **Privilèges (onglet)** > **Privilèges de mise à jour des composants**.

  b. Demandez aux utilisateurs de mettre à jour manuellement les composants sur le endpoint de l'agent (en cliquant avec le bouton droit de la souris sur l'icône de l'agent OfficeScan dans la barre d'état système, puis avec le bouton gauche sur « Mettre à jour ») pour obtenir les paramètres de configuration mis à jour.

Lorsque des agents OfficeScan sont mis à jour, ils reçoivent à la fois les composants et les fichiers de configuration mis à jour.

Utilisation de l'outil de mise à jour programmée des domaines

La programmation des mises à jour configurée dans les mises à jour automatiques des agents concerne uniquement les agents disposant de privilèges de mise à jour programmée. Pour les autres agents, vous pouvez définir une programmation des mises à jour distincte. Pour cela, configurez une programmation par domaines de l'arborescence des agents. Tous les agents appartenant à un même domaine seront soumis à cette programmation.



Remarque

Il n'est pas possible de définir une programmation de mises à jour pour un agent ou un sous-domaine spécifique. Tous les sous-domaines sont soumis à la programmation configurée pour leur domaine parent.

Procédure

1. Prenez note du nom des domaines de l'arborescence des agents et des programmations de mises à jour.
2. Accédez au répertoire <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\DomainScheduledUpdate`.
3. Copiez les fichiers suivants dans `<Dossier d'installation du serveur>\PCCSRV` :
    - `DomainSetting.ini`
    - `dsu_convert.exe`
4. Ouvrez `DomainSetting.ini` à l'aide d'un éditeur de texte comme le Bloc-notes.
5. Indiquez un domaine de l'arborescence des agents, puis configurez la programmation des mises à jour pour ce domaine. Répétez cette étape pour ajouter d'autres domaines.

    Remarque

    Des instructions de configuration détaillées sont indiquées dans le fichier `.ini`.

6. Enregistrez le fichier `DomainSetting.ini`.
7. Ouvrez une invite de commande et accédez au répertoire du dossier `PCCSRV`.
8. Entrez la commande suivante, puis appuyez sur `Entrée`.

    `dsuconvert.exe DomainSetting.ini`

9. Sur la console Web, accédez à **Agents** > **Paramètres de l'agent général**.

10. Cliquez sur **Enregistrer**.

Mises à jour manuelles des agents OfficeScan

Mettez à jour manuellement les composants des agents OfficeScan lorsqu'ils sont particulièrement obsolètes et en cas d'épidémie. Les composants des agents OfficeScan deviennent particulièrement obsolètes lorsqu'un agent OfficeScan ne parvient pas à mettre à jour les composants depuis la source de mise à jour pendant une période prolongée.

Outre les mises à jour de composants, les agents OfficeScan reçoivent automatiquement des fichiers de configuration mis à jour lors d'une mise à jour manuelle. Les agents OfficeScan ont besoin des fichiers de configuration pour appliquer les nouveaux paramètres. À chaque fois que vous modifiez les paramètres d'OfficeScan via la console Web, les fichiers de configuration sont modifiés.



Remarque

En plus de lancer des mises à jour manuelles, vous pouvez accorder aux utilisateurs le privilège d'exécuter ces mises à jour (option également appelée **Mettre à jour** sur les endpoints des agents OfficeScan). Pour obtenir des informations détaillées, voir *Configuration des privilèges de mise à jour et d'autres paramètres à la page 6-51*.

Mise à jour manuelle des agents OfficeScan

Procédure

1. Accédez à **Mises à jour** > **Agents** > **Mise à jour manuelle**.

2. Les composants actuellement disponibles sur le serveur OfficeScan et la date de dernière mise à jour de ces composants s'affichent en haut de l'écran. Assurez-vous que les composants sont à jour avant de demander aux agents d'effectuer une mise à jour.



Remarque

Mettez à jour manuellement les composants obsolètes sur le serveur. Voir *Mises à jour manuelles des agents OfficeScan à la page 6-49* pour obtenir des informations détaillées.

3. Pour mettre à jour uniquement les agents ayant des composants obsolètes :

    a. Cliquez sur **Sélectionner les agents dont les composants sont obsolètes**.

    b. (Facultatif) Sélectionnez **Inclure le ou les agents itinérants et hors ligne** :

        - Pour mettre à jour les agents itinérants ayant une connexion opérationnelle avec le serveur.

        - Pour mettre à jour les agents hors ligne lorsqu'ils sont à nouveau en ligne.

    c. Cliquez sur **Lancer la mise à jour**.



Remarque

Le serveur recherche les agents dont les versions des composants sont antérieures à celles du serveur, puis demande à ces agents d'effectuer une mise à jour. Pour vérifier l'état de la notification, accédez à l'écran **Mises à jour** > **Résumé**.

4. Pour mettre à jour les agents de votre choix :

    a. Sélectionnez **Sélectionner manuellement les agents**.

    b. Cliquez sur **Sélectionner**.

    c. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.

    d. Cliquez sur **Lancer la mise à jour des composants**.



Remarque

Le serveur commence à demander à chaque agent de télécharger les composants mis à jour. Pour vérifier l'état de la notification, accédez à l'écran **Mises à jour** > **Résumé**.

Configuration des privilèges de mise à jour et d'autres paramètres

Configurez les paramètres de mise à jour et accordez aux utilisateurs des agents certains privilèges, tels que l'exécution de la fonction « Mettre à jour » et l'activation d'une mise à jour programmée.

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Cliquez sur l'onglet **Autres paramètres** et configurez les options suivantes dans la section **Paramètres de mise à jour**.

Option	Description
Les agents OfficeScan téléchargent des mises à jour depuis le serveur ActiveUpdate de Trend Micro	Lorsque des mises à jour sont lancées, les agents OfficeScan les obtiennent tout d'abord depuis la source de mise à jour spécifiée dans l'écran **Mises à jour** > **Agents** > **Source de mise à jour** Si la mise à jour échoue, les agents essaient de procéder à la mise à jour à partir du serveur OfficeScan. La sélection de cette option permet aux agents de tenter une mise à jour depuis le serveur ActiveUpdate de Trend Micro si la mise à jour depuis le serveur OfficeScan échoue. **Remarque** Un agent IPv6 pur ne peut pas directement effectuer de mise à jour à partir du serveur ActiveUpdate de Trend Micro. Un serveur proxy à double pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre aux agents de se connecter au serveur ActiveUpdate.
Activer les mises à jour programmée s sur les	La sélection de cette option configure tous les agents OfficeScan afin qu'ils activent les mises à jour programmées par défaut. Les utilisateurs disposant du privilège **Activer/Désactiver les mises à jour programmées** peuvent modifier ce paramètre.

OPTION	DESCRIPTION
agents OfficeScan	Pour plus de détails sur la configuration de la mise à jour programmée, voir *Configuration des mises à jour automatiques des agents OfficeScan à la page 6-44*.
Les agents OfficeScan peuvent mettre à jour les composants, mais ne peuvent pas mettre à niveau le programme de l'agent, ni déployer des correctifs de type hot fix	Cette option permet d'effectuer les mises à jour de composants, mais empêche le déploiement des correctifs de type hot fix et la mise à niveau des agents OfficeScan. **Remarque** La désactivation de cette option peut affecter de manière négative les performances du serveur, car cela signifie que tous les agents se connectent simultanément au serveur pour procéder à une mise à niveau ou à l'installation d'un correctif de type hot fix.

5. Cliquez sur l'onglet **Privilèges** et configurez les options suivantes dans la section **Mises à jour des composants** :

OPTION	DESCRIPTION
Exécuter l'option « Mettre à jour »	Les utilisateurs disposant de ce privilège peuvent mettre à jour les composants à la demande en cliquant avec le bouton droit sur l'icône due l'agent OfficeScan dans la barre d'état système et en sélectionnant **Mettre à jour**. **Remarque** Les utilisateurs des agents OfficeScan peuvent utiliser des paramètres proxy lors de l'exécution de l'option « Mettre à jour ». Voir *Privilèges de configuration proxy pour les agents à la page 14-53* pour obtenir des informations détaillées.
Activer/ Désactiver les mises à jour	La sélection de cette option permet aux utilisateurs des agents OfficeScan d'activer ou de désactiver les mises à jour programmées à l'aide du menu contextuel (accessible avec le bouton droit de la souris) de l'agent OfficeScan, qui peut prendre

OPTION	DESCRIPTION
programmée s	le pas sur le paramètre **Activer les mises à jour programmées sur les agents OfficeScan**. **Remarque** Les administrateurs doivent sélectionner le paramètre **Activer les mises à jour programmées sur les agents OfficeScan** dans l'onglet **Autres paramètres** avant que cette option de menu n'apparaisse dans le menu de l'agent OfficeScan.

6. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :

   - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.

   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Configuration de l'espace disque réservé pour les mises à jour des agents OfficeScan

OfficeScan attribue une certaine quantité d'espace disque sur les agents pour les correctifs de type hot fix, les fichiers de signatures, les moteurs de scan et les mises à jour des programmes. Par défaut, OfficeScan réserve 60 Mo d'espace disque.

Procédure

1. Accédez à **Agents** > **Paramètres généraux de l'agent**.
2. Accédez à la section **Espace disque réservé**.
3. Sélectionnez **Réserver __ Mo d'espace disque pour les mises à jour**.

4. Sélectionnez le volume d'espace disque.

5. Cliquez sur **Enregistrer**.

Proxy pour les mises à jour des composants des agents OfficeScan

Les agents OfficeScan utilisent des paramètres proxy pendant la mise à jour automatique ou s'ils sont autorisés à exécuter l'option « Mettre à jour ».

Tableau 6-9. Paramètres proxy utilisés pendant les mises à jour des composants des agents OfficeScan

Méthode de mise à jour	Paramètres proxy utilisés	Utilisation
Mise à jour automatique	• Paramètres proxy automatiques. Pour obtenir des informations détaillées, voir *Paramètres proxy automatiques pour les agents OfficeScan à la page 14-55*. • Paramètres proxy interne. Pour obtenir des informations détaillées, voir *Proxy interne pour les agents OfficeScan à la page 14-51*.	1. Les agents OfficeScan utilisent en priorité les paramètres proxy automatiques pour la mise à jour des composants. 2. Si les paramètres proxy automatiques ne sont pas activés, les paramètres proxy interne sont utilisés. 3. Si les deux sont désactivés, les agents n'utilisent pas de paramètres proxy.

Méthode de mise à jour	Paramètres proxy utilisés	Utilisation
Mettre à jour	• Paramètres proxy automatiques. Pour obtenir des informations détaillées, voir *Paramètres proxy automatiques pour les agents OfficeScan à la page 14-55*. • Paramètres proxy configurés par l'utilisateur. Vous pouvez accorder aux utilisateurs d'agents l'autorisation de configurer les paramètres proxy. Pour obtenir des informations détaillées, voir *Privilèges de configuration proxy pour les agents à la page 14-53*.	1. Les agents OfficeScan utilisent en priorité les paramètres proxy automatiques pour la mise à jour des composants. 2. Si les paramètres proxy automatiques ne sont pas activés, les paramètres proxy configurés par l'utilisateur sont utilisés. 3. Si les deux sont désactivés ou si les paramètres proxy automatiques sont désactivés alors que les utilisateurs des agents ne disposent pas du privilège requis, les agents n'utilisent pas de proxy lors de la mise à jour des composants.

Configuration des notifications de mise à jour des agents OfficeScan

OfficeScan notifie les utilisateurs des agents lorsque des événements associés à la mise à jour se produisent.

Procédure

1. Accédez à **Agents** > **Paramètres généraux de l'agent**.
2. Rendez-vous à la section **Paramètres d'alerte**.
3. Sélectionnez les options suivantes :

- **Afficher l'icône d'alerte dans la barre des tâches Windows si le fichier de signatures de virus n'a pas été mis à jour au bout de __ jour(s)** : Une icône d'alerte s'affiche dans la barre des tâches Windows pour rappeler aux utilisateurs de mettre à jour un fichier de signatures de virus n'ayant pas été mis à jour durant la période indiquée. Pour mettre à jour le fichier de signatures, utilisez l'une des méthodes de mise à jour indiquées dans *Méthodes de mise à jour des agents OfficeScan à la page 6-41*.

  Tous les agents gérés par le serveur appliqueront ce paramètre.

- **Afficher un message de notification si le endpoint doit être redémarré pour charger un pilote en mode noyau** : après l'installation d'un correctif de type hot fix ou d'un package de mise à niveau contenant une nouvelle version d'un pilote en mode noyau, la version précédente du pilote est susceptible d'être toujours présente sur le endpoint. Le seul moyen de décharger la version précédente et de charger la nouvelle est de redémarrer le endpoint. Une fois le endpoint redémarré, la nouvelle version est automatiquement installée et aucun redémarrage n'est nécessaire.

  Le message de notification s'affiche immédiatement après l'installation, par le endpoint de l'agent, du correctif de type hot fix ou du package de mise à niveau.

4. Cliquez sur **Enregistrer**.

Affichage des journaux de mise à jour des agents OfficeScan

Consultez les journaux de mise à jour des agents pour déterminer s'il existe des problèmes de mise à jour du fichier de signatures de virus sur les agents.



Remarque

Dans cette version du produit, seuls les journaux de mise à jour des fichiers de signatures de virus peuvent être interrogés depuis la console Web.

Pour éviter que les journaux n'occupent trop d'espace sur votre disque dur, vous pouvez les supprimer manuellement ou configurer leur suppression programmée. Voir *Gestion du*

journal à la page 13-36 pour obtenir des informations complémentaires sur la gestion des journaux.

Procédure

1. Accédez à **Journaux** > **Agents** > **Mise à jour des composants de l'agent**.
2. Pour afficher le nombre de mises à jour des agents, cliquez sur **Afficher** dans la colonne **Progression**. L'écran **Progression de la mise à jour des composants** s'affiche ; il indique le nombre d'agents mis à jour toutes les 15 minutes, ainsi que le nombre total d'agents mis à jour.
3. Pour afficher les agents ayant mis à jour le fichier de signatures de virus, cliquez sur **Afficher** dans la colonne **Détails**.
4. Pour sauvegarder les journaux dans un fichier CSV (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Application des mises à jour des agents OfficeScan

Utilisez la conformité de la sécurité pour garantir que les agents disposent des composants les plus récents. La conformité de la sécurité détermine les incohérences des versions des composants entre le serveur et les agents OfficeScan. Ces incohérences se produisent généralement lorsque les agents ne peuvent pas se connecter au serveur pour mettre à jour les composants. Si l'agent obtient une mise à jour d'une autre source (telle que le serveur ActiveUpdate), il est possible qu'un composant de l'agent soit plus récent que celui du serveur.

Pour plus d'informations, voir *Conformité de la sécurité pour les agents gérés à la page 14-59*.

Rétrogradation des composants des agents OfficeScan

Rétrograder signifie revenir à une version précédente du fichier de signatures de virus, du fichier Smart Scan Agent Pattern et du moteur de scan antivirus. Si ces composants ne fonctionnent pas correctement, rétrogradez-les vers leur version précédente. OfficeScan conserve les versions actuelles et précédentes du moteur de scan antivirus et

les cinq dernières versions du fichier de signatures de virus et du fichier Smart Scan Agent Pattern.



Remarque

Seuls les composants mentionnés ci-dessus peuvent être rétrogradés.

OfficeScan utilise des moteurs de scan différents pour les agents exécutant des plates-formes 32 bits et 64 bits. Il est nécessaire de rétrograder ces moteurs de scan séparément. La procédure de rétrogradation est identique pour tous les types de moteurs.

Procédure

1. Accédez à **Mises à jour** > **Rétrograder**.
2. Cliquez sur **Synchroniser avec le serveur** dans la section appropriée.
    a. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
    b. Cliquez sur **Rétrograder**.
    c. Cliquez sur **Afficher journaux de mise à jour** pour vérifier le résultat ou **Retour** pour revenir à l'écran Rétrograder.
3. Si une version antérieure du fichier de signatures existe sur le serveur, cliquez sur **Rétrograder le serveur et les agents** pour rétrograder les fichiers de signatures de l'agent et du serveur OfficeScan.

Exécution de l'outil Touch Tool pour les correctifs de type hot fix des agents OfficeScan

L'outil Touch Tool synchronise l'horodatage d'un fichier grâce avec celui d'un autre ou de l'horloge système du endpoint. Si vous ne parvenez pas à déployer un correctif de type hotfix sur le serveur OfficeScan, utilisez Touch Tool pour changer l'horodatage du correctif de type hotfix. OfficeScan considère alors qu'il s'agit d'un nouveau correctif de

type hotfix, ce qui amène le serveur à tenter automatiquement un nouveau déploiement du correctif.

Procédure

1. Sur le serveur OfficeScan, accédez au répertoire <*dossier d'installation du serveur*> `\PCCSRV\Admin\Utility\Touch`.

2. Copiez le fichier `TMTouch.exe` dans le dossier contenant le fichier à modifier. Si vous synchronisez l'horodatage d'un fichier grâce à celui d'un autre fichier, placez les deux fichiers dans l'emplacement de l'outil Touch Tool.

3. Ouvrez une invite de commande et accédez à l'emplacement de l'outil Touch Tool.

4. Entrez ce qui suit :

   ```
   TmTouch.exe <nom du fichier de destination> <nom du fichier source>
   ```

   Où :

   - `<nom du fichier de destination>` est le nom de fichier du correctif de type hot fix dont vous voulez changer l'horodatage
   - `<nom du fichier source>` est le nom du fichier dont vous voulez répliquer l'horodatage

   Remarque

   Si vous ne définissez pas de nom de fichier source, l'outil définit l'horodatage du fichier de destination en fonction de l'heure du système du endpoint. Utilisez le caractère générique (*) pour le fichier de destination, mais pas pour le nom du fichier source.

5. Pour vérifier que l'horodatage a bien été modifié, saisissez `dir` dans l'invite de commande ou vérifiez les propriétés du fichier dans l'Explorateur Windows.

Agents de mise à jour

Pour distribuer la tâche de déploiement des composants, des paramètres de domaine ou des programmes des agents et des correctifs de type hot fix vers les agents OfficeScan, attribuez à certains agents OfficeScan le rôle d'agents de mise à jour, ou de sources de mise à jour pour les autres agents. Cela permet de s'assurer que les agents reçoivent des mises à jour en temps et en heure, évitant au serveur OfficeScan d'avoir à gérer un trafic réseau trop important.

Si le réseau est segmenté par sites et si le lien réseau entre les segments présente un trafic élevé, affectez au moins un agent de mise à jour à chaque site.



Remarque

Les agents OfficeScan configurés pour mettre à jour leurs composants depuis un agent de mise à jour reçoivent uniquement des composants et des paramètres mis à jour de l'agent de mise à jour. Tous les agents OfficeScan dépendent toujours du serveur OfficeScan.

Configuration minimale requise pour les agents de mise à jour

Visitez le site Web suivant pour obtenir la liste complète des configurations requises :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Configuration de l'agent de mise à jour

La configuration de l'agent de mise à jour s'effectue en 2 étapes:

1. Affectez un agent OfficeScan en tant qu'agent de mise à jour de composants spécifiques.

2. Spécifiez les agents qui seront mis à jour à partir de cet agent de mise à jour.



Remarque

Le nombre de connexions d'agent simultanées qu'un agent de mise à jour peut gérer dépend des spécifications matérielles du endpoint.

Attribution à des agents OfficeScan du rôle d'agent de mise à jour

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, sélectionnez les agents qui seront désignés en tant qu'agents de mise à jour.

   Remarque

   Il n'est pas possible de sélectionner l'icône du domaine racine puisque tous les agents seraient alors désignés comme agents de mise à jour. Un agent de mise à jour IPv6 our ne peut pas distribuer des mises à jour directement à des agents IPv4 purs. De même, un agent de mise à jour IPv4 pur ne peut pas distribuer des mises à jour directement à des agents IPv6 purs. Un serveur proxy à double pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre à l'agent de mise à jour de distribuer des mises à jour aux agents.

3. Cliquez sur **Paramètres** > **Paramètres des agents de mise à jour**.
4. Sélectionnez les éléments que les agents de mise à jour peuvent partager.
   - Mises à jour des composants
   - Paramètres de domaine
   - Programmes et correctifs de type hot fix des agents OfficeScan
5. Cliquez sur **Enregistrer**.

Spécification des agents OfficeScan mis à jour par un agent de mise à jour

Procédure

1. Accédez à **Mises à jour** > **Agents** > **Source de mise à jour**.
2. Sous **Liste des sources de mise à jour personnalisées**, cliquez sur **Ajouter**.
3. Dans l'écran qui s'affiche, indiquez les adresses IP des agents. Vous pouvez entrer une plage d'adresses IPv4 et/ou un préfixe IPv6 et sa longueur.
4. Dans le champ **Agent de mise à jour**, sélectionnez l'agent de mise à jour que vous voulez attribuer aux agents.



Remarque

Assurez-vous que les agents peuvent se connecter à l'agent de mise à jour en utilisant leurs adresses IP. Par exemple, si vous avez spécifié une plage d'adresses IPv4, l'agent de mise à jour doit avoir une adresse IPv4. Si vous avez spécifié un préfixe IPv6 et une longueur de préfixe, l'agent de mise à jour doit comporter une adresse IPv6.

5. Cliquez sur **Enregistrer**.

Sources de mises à jour pour les agents de mises à jour

Les agents de mise à jour peuvent obtenir des mises à jour à partir de sources diverses, telles que le serveur OfficeScan ou à partir d'une source personnalisée. Configurez la source de mise à jour à partir de l'écran de source de mise à jour de la console Web.

Prise en charge d'IPv6 pour les agents de mise à jour

Un agent de mise à jour IPv6 pur ne peut effectuer directement de mises à jour à partir de sources de mise à jour IPv4 pures, telles que :

- un serveur OfficeScan IPv4 pur
- Toute source de mise à jour personnalisée IPv4 pure

- Trend Micro ActiveUpdate server

De même, un agent de mise à jour IPv4 pur ne peut pas effectuer de mises à jour à partir de sources de mise à jour IPv6 pur, telles qu'un serveur OfficeScan IPv6 pur.

Un serveur proxy double-pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre aux agents de mise à jour de se connecter aux sources de mise à jour.

Source de mise à jour standard pour les agents de mise à jour

Le serveur OfficeScan est la source de mise à jour standard pour les agents de mise à jour. Si vous configurez des agents pour la mise à jour directe à partir du serveur OfficeScan, le processus de mise à jour s'effectue de la façon suivante :

1. L'agent de mise à jour obtient les mises à jour à partir du serveur OfficeScan.
2. S'il ne peut pas être mis à jour à partir du serveur OfficeScan, l'agent tente de se connecter directement à Trend Micro ActiveUpdate Server si l'une des conditions suivantes est remplie :
    - Sous **Agents** > **Gestion des agents**, puis sous **Paramètres** > **Privilèges et autres paramètres** > **Autres paramètres** > **Paramètres de mise à jour**, l'option **Les agents OfficeScan téléchargent des mises à jour depuis le serveur ActiveUpdate de Trend Micro** est activée.
    - Le serveur ActiveUpdate est la première entrée de la liste de sources de mise à jour personnalisées.



Conseil

Ne placez le serveur ActiveUpdate en haut de la liste que si vous rencontrez des problèmes de mise à jour à partir du serveur OfficeScan. Lorsque les agents de mise à jour effectuent la mise à jour directe à partir du serveur ActiveUpdate, ils consomment une portion significative de la bande passante réseau et Internet.

3. S'il ne peut pas obtenir les mises à jour à partir des sources possibles, l'agent de mise à jour abandonne le processus de mise à jour.

Sources de mises à jour personnalisées pour les agents de mises à jour

En plus du serveur OfficeScan, les agents de mise à jour peuvent effectuer la mise à jour depuis des sources de mise à jour personnalisées. Les sources de mise à jour personnalisées contribuent à la réduction du trafic de mise à jour des agents dirigé vers le serveur OfficeScan. Spécifiez les sources de mise à jour personnalisées dans la Liste de sources de mise à jour personnalisées, qui peut accueillir jusqu'à 1024 sources de mise à jour. Voir *Sources de mise à jour personnalisées pour les agents OfficeScan à la page 6-36* pour connaître les étapes de configuration de la liste.



Remarque

Assurez-vous que l'option **Les agents de mise à jour effectuent la mise à jour des composants, des paramètres du domaine, des programmes des agents et des correctifs de type hot fix, uniquement à partir du serveur OfficeScan** est désactivée sur l'écran **Source de mise à jour pour les agents** (**Mises à jour** > **Agents** > **Source de mise à jour**) afin que les agents de mise à jour puissent se connecter aux sources de mise à jour personnalisées.

Après avoir défini et enregistré la liste, le processus de mise à jour s'effectue de la façon suivante :

1. L'agent de mise à jour effectue la mise à jour à partir de la première entrée de la liste.

2. S'il ne peut pas effectuer la mise à jour à partir de la première entrée, il essaie avec la seconde entrée, et ainsi de suite.

3. Si l'agent ne parvient à effectuer la mise à jour à partir d'aucune des entrées, il vérifie les options suivantes sous l'en-tête **Les agents OfficeScan mettent à jour les éléments suivants à partir du serveur OfficeScan si toutes les sources personnalisées sont indisponibles ou introuvables** :

   - **Composants** : Si l'option est activée, l'agent effectue la mise à jour à partir du serveur OfficeScan.

     Si l'option est désactivée, l'agent essaie ensuite de se connecter directement à Trend Micro ActiveUpdate Server si l'une des conditions suivantes est remplie :



Remarque

Vous ne pouvez mettre à jour des composants qu'à partir du serveur Active Update. Les paramètres de domaine, les programmes et les correctifs de type hot fix ne peuvent être téléchargés qu'à partir du serveur ou des agents de mise à jour.

  - Sous **Agents** > **Gestion des agents**, puis sous **Paramètres** > **Privilèges et autres paramètres** > **Autres paramètres** > **Paramètres de mise à jour**, l'option **Les agents téléchargent des mises à jour depuis le serveur ActiveUpdate de Trend Micro** est activée.
  - Le serveur ActiveUpdate n'est pas inclus dans la liste de sources de mise à jour personnalisées.
- **Paramètres de domaine** : Si l'option est activée, l'agent effectue la mise à jour à partir du serveur OfficeScan.
- **Programmes et correctifs de type hot fix des agents OfficeScan** : Si l'option est activée, l'agent effectue la mise à jour à partir du serveur OfficeScan.

4. S'il ne peut pas obtenir les mises à jour à partir des sources possibles, l'agent de mise à jour abandonne le processus de mise à jour.

Le processus de mise à jour est différent si l'option **Source de mise à jour standard (mise à jour depuis le serveur OfficeScan)** est activée et si le serveur OfficeScan notifie l'agent de la nécessité de mettre à jour les composants. Le processus est le suivant :

1. L'agent effectue la mise à jour directement à partir du serveur OfficeScan et ignore la liste des sources de mise à jour.
2. S'il ne peut pas être mis à jour à partir du serveur, l'agent tente de se connecter directement à Trend Micro ActiveUpdate Server si l'une des conditions suivantes est remplie :
   - Sous **Agents** > **Gestion des agents**, puis sous **Paramètres** > **Privilèges et autres paramètres** > **Autres paramètres** > **Paramètres de mise à jour**, l'option **Les agents OfficeScan téléchargent des mises à jour depuis le serveur ActiveUpdate de Trend Micro** est activée.

- Le serveur ActiveUpdate est la première entrée de la liste de sources de mise à jour personnalisées.



Conseil

Ne placez le serveur ActiveUpdate en haut de la liste que si vous rencontrez des problèmes de mise à jour à partir du serveur OfficeScan. Lorsque des agents OfficeScan effectuent la mise à jour directement depuis le serveur ActiveUpdate, ils consomment une portion significative de la bande passante réseau et Internet.

3. S'il ne peut pas obtenir les mises à jour à partir des sources possibles, l'agent de mise à jour abandonne le processus de mise à jour.

Configuration de la source de mise à jour pour l'agent de mise à jour

Procédure

1. Accédez à **Mises à jour** > **Agents** > **Source de mise à jour**.
2. Choisissez d'effectuer la mise à jour à partir de la source de mise à jour standard pour les agents de mise à jour (serveur OfficeScan) ou de la source de mise à jour personnalisée pour les agents de mise à jour.
3. Cliquez sur **Notifier tous les agents**.

Duplication des composants d'un agent de mise à jour

les agents de mise à jour utilisent la duplication des composants lors du téléchargement des composants, tout comme le fait le serveur OfficeScan. Voir *Duplication des composants du serveur OfficeScan à la page 6-23* pour plus d'informations sur la manière dont le serveur effectue la duplication des composants.

Le processus de duplication des composants pour les agents de mise à jour est le suivant :

1. L'agent de mise à jour compare la version actuelle de son fichier de signatures complet avec la dernière version disponible depuis la source de mise à jour. Si la

différence entre les deux versions est inférieure ou égale à 14, l'agent de mise à jour ne télécharge que le fichier de signatures incrémentiel qui correspond à la différence entre les deux versions.



Remarque

Si la différence est supérieure à 14, l'agent de mise à jour télécharge automatiquement la version complète du fichier de signatures.

2. L'agent de mise à jour fusionne le fichier de signatures incrémentiel qu'il a téléchargé avec son fichier de signatures complet actuel pour générer le fichier de signatures complet le plus récent.

3. L'agent de mise à jour télécharge tous les fichiers de signatures incrémentiels restants depuis la source de mise à jour.

4. Le dernier fichier de signatures complet et tous les fichiers de signatures incrémentiels sont mis à la disposition des agents.

Méthodes de mise à jour pour les agents de mise à jour

Les agents de mise à jour utilisent des méthodes de mise à jour identiques à celles qu'utilisent les agents ordinaires. Pour obtenir des informations détaillées, voir *Méthodes de mise à jour des agents OfficeScan à la page 6-41*.

Vous pouvez également utiliser l'outil de configuration des mises à jour programmées pour activer et configurer les mises à jour programmées sur un agent de mise à jour installé à l'aide d'Agent Packager.



Remarque

Cet outil n'est pas disponible si l'agent de mise à jour a été installé avec une autre méthode. Voir la *Éléments à prendre en compte pour le déploiement à la page 5-11* pour plus d'informations.

Utilisation de l'outil de configuration de mise à jour programmée

Procédure

1. Sur le endpoint de l'agent de mise à jour, accédez au répertoire <*dossier d'installation de l'agent*>.
2. Double-cliquez sur le fichier `SUCTool.exe` pour exécuter l'outil. La console de l'outil de configuration des mises à jour programmées s'ouvre.
3. Sélectionnez **Activer la mise à jour programmée**.
4. Spécifiez la fréquence et l'heure de mise à jour.
5. Cliquez sur **Appliquer**.

Rapport d'analyse de l'agent de mise à jour

Générez le rapport d'analyse de l'agent de mise à jour pour analyser l'infrastructure de mise à jour et déterminer quels agents effectuent des téléchargements à partir du serveur OfficeScan, des agents de mise à jour ou du serveur ActiveUpdate. Ce rapport vous permet également de vérifier si le nombre d'agents demandant des mises à jour à partir des sources de mise à jour dépasse les ressources disponibles, et de rediriger le trafic réseau vers les sources appropriées.



Remarque

Ce rapport englobe tous les agents de mise à jour. Si vous avez délégué la tâche de gestion d'un ou plusieurs domaines à d'autres administrateurs, ceux-ci visualisent également les agents de mise à jour appartenant aux domaines qu'ils ne gèrent pas.

OfficeScan exporte le Rapport d'analyse de l'agent de mise à jour dans un fichier de valeurs séparées par des virgules (`.csv`).

Ce rapport contient les informations suivantes :

- Endpoint de l'agent OfficeScan

- adresse IP
- Chemin d'accès de l'arborescence des agents
- Source de mise à jour
- Si les agents téléchargent ce qui suit à partir des agents de mise à jour :
    - Composants
    - Paramètres de domaine
    - Programmes et correctifs de type hot fix des agents OfficeScan



Important

Le rapport d'analyse de l'agent de mise à jour répertorie uniquement les agents OfficeScan configurés pour recevoir des mises à jour partielles de l'agent de mise à jour. Les agents OfficeScan configurés pour recevoir des mises à jour complètes d'un agent de mise à jour (y compris les composants, paramètres de domaine, programmes de l'agent OfficeScan et correctifs de type hot fix) ne figurent pas dans le rapport.

Pour plus de détails sur la génération du rapport, reportez-vous à *Sources de mise à jour personnalisées pour les agents OfficeScan à la page 6-36*.

Résumé des mises à jour de composants

La console Web comporte un écran **Résumé des mises à jour** (accédez à **Mises à jour** > **Résumé**) qui vous informe de l'état général des mises à jour des composants et vous permet de mettre à jour les composants obsolètes. Si vous activez la mise à jour programmée du serveur, l'écran affichera également la prochaine mise à jour programmée.

Actualisez périodiquement l'écran pour afficher l'état le plus récent de mise à jour des composants.



Remarque

Pour afficher les mises à jour des composants sur le serveur Smart Protection Server intégré, accédez à **Administration** > **Smart Protection** > **Serveur intégré**.

État de la mise à jour des agents OfficeScan

Si vous avez lancé la mise à jour des composants sur les agents, consultez les informations suivantes dans cette section :

- Nombre d'agents informés de la mise à jour des composants à effectuer.
- Nombre d'agents non informés mais déjà dans la file d'attente des notifications. Pour annuler l'envoi de la notification à ces agents, cliquez sur **Annuler la notification**.

Composants

Dans le tableau **État de mise à jour**, vous pouvez afficher l'état de mise à jour de chaque composant que le serveur OfficeScan télécharge et distribue.

La version actuelle et la date de dernière mise à jour de chaque composant sont affichées. Cliquez sur le lien numéroté pour afficher les agents dont des composants sont obsolètes. Mettez à jour manuellement les agents dont des composants sont obsolètes.



Chapitre 7

Recherche des risques de sécurité

Ce chapitre explique comment protéger les ordinateurs des risques de sécurité en utilisant le scan de fichiers.

Les rubriques sont les suivantes :

À propos des risques de sécurité

« Risque de sécurité » est le terme générique regroupant les virus/programmes malveillants et les spywares/grayware. OfficeScan protège les ordinateurs contre les risques de sécurité en scannant les fichiers avant de mener une action spécifique selon chaque risque détecté. Un nombre élevé de risques de sécurité détectés en peu de temps témoigne d'une épidémie. OfficeScan OfficeScan peut aider à enrayer les épidémies en appliquant des stratégies de prévention des épidémies et en isolant les ordinateurs sur lesquels sont détectés les fichiers infectés jusqu'à ce qu'ils ne présentent plus aucun risque. Des notifications et des journaux vous aident à vous tenir informé des risques de sécurité tout en vous alertant lorsqu'une action immédiate s'impose.

Virus et programmes malveillants

Il existe des dizaines de milliers de virus/programmes malveillants et de nouveaux sont créés chaque jour. Alors que par le passé, ils étaient plus courants dans DOS ou Windows, les virus informatiques de notre époque peuvent provoquer des dommages importants sur les endpoints en exploitant les vulnérabilités de sécurité des réseaux d'entreprise, des systèmes de messagerie électronique et des sites Web.

Tableau 7-1. Type de virus/programmes malveillants

Type de virus/ programmes malveillants	Description
Canular	Les canulars sont des programmes similaires à des virus, qui manipulent généralement l'apparence des objets sur l'écran du endpoint.
Autres	« Autres » inclut les virus/programmes malveillants n'entrant dans aucune autre catégorie de virus ou programmes malveillants.
Utilitaire de compression	Désigne un programme exécutable compressé et/ou chiffré Windows ou Linux™, souvent un cheval de Troie. La compression de fichiers exécutables rend l'utilitaire de compression plus difficile à détecter par les logiciels antivirus.

Type de virus/ programmes malveillants	Description
Rootkit	Les rootkits sont des programmes (ou des ensembles de programmes) qui installent et exécutent un code sur un système à l'insu de l'utilisateur et sans son autorisation. Ils utilisent une technique de camouflage pour maintenir une présence persistante et indétectable sur la machine. Les rootkits n'infectent pas les machines. Ils cherchent plutôt à fournir un environnement indétectable afin d'exécuter un code malveillant. Les rootkits sont installés sur les systèmes via un piratage psychologique, lors de l'exécution de programmes malveillants ou simplement en naviguant sur un site Web malveillant. Une fois installé, un pirate peut pratiquement effectuer n'importe quelle action sur le système, notamment l'accès à distance et l'espionnage. Il peut également masquer des processus, des fichiers, des clés de registre et des canaux de communication.
Virus de test	Les virus de test sont des fichiers inertes qui agissent comme un véritable virus et qui peuvent être détectés par les logiciels antivirus. Utilise des virus de test tels que le script de test EICAR afin de vérifier que le scan de votre installation antivirus fonctionne correctement.
Cheval de Troie	Les chevaux de Troie utilisent souvent les ports pour accéder aux ordinateurs ou aux programmes exécutables. Les programmes Cheval de Troie ne se répliquent pas, mais résident dans des systèmes pour effectuer des opérations malveillantes, telles que l'ouverture des ports aux pirates. Les solutions antivirus conventionnelles peuvent détecter et supprimer les virus, mais pas les chevaux de Troie, notamment ceux qui ont déjà pénétré votre système.

Type de virus/ programmes malveillants	Description
Virus	Les virus sont des programmes capables de se répliquer. Pour ce faire, le virus doit s'attacher à d'autres fichiers programmes et s'exécuter chaque fois que le programme hôte est lancé. • **Code malicieux ActiveX** : Code résidant dans les pages Web qui exécutent des contrôles ActiveX™ • **Virus du secteur d'amorçage** : Virus qui infecte le secteur d'amorçage d'une partition ou d'un disque. • **Virus infectant les fichiers COM et EXE** : Programme exécutable avec extensions `.com` ou `.exe` • **Code malveillant Java** : Virus indépendant du système d'exploitation écrit ou imbriqué dans Java™. • **Virus de macro** : Virus chiffré comme application macro qui est souvent inclus à un document. • Virus **VBScript**, **JavaScript** ou **HTML** : Réside sur des pages Web et est téléchargé par un navigateur. • **Vers** : Programme automatique ou ensemble de programmes pouvant répandre des copies fonctionnelles de lui-même ou de ses segments sur les systèmes d'autres endpoints, souvent par le biais de courrier électronique.
Virus de réseau	Un virus qui se répand sur le réseau n'est pas, à proprement parler, un virus de réseau. Seuls certains des types virus/programmes malveillants, comme les vers, peuvent être appelés virus de réseau. Plus spécifiquement, les virus de réseau utilisent les protocoles réseau tels que TCP, FTP, UDP, HTTP et les protocoles d'e-mail pour se multiplier. Souvent, ils n'affectent pas les fichiers système ou ne modifient pas les secteurs d'amorçage des disques durs. Par contre, les virus de réseau infectent la mémoire des ordinateurs des agents, en les obligeant à submerger le réseau de trafic, ce qui peut entraîner des ralentissements, voire même une panne complète du réseau. Comme les virus de réseau restent en mémoire, ils sont souvent indétectables par les méthodes conventionnelles de scan de fichiers basées sur l'E/S.

TYPE DE VIRUS/ PROGRAMMES MALVEILLANTS	DESCRIPTION
Virus/ programmes malveillants probables	Les virus/programmes malveillants probables sont des fichiers suspects ayant certaines des caractéristiques d'un virus/programme malveillant. Pour plus d'informations, consultez l'Encyclopédie des virus de Trend Micro : http://www.trendmicro.com/vinfo/fr/virusencyclo/default.asp **Remarque** Le nettoyage ne peut pas être effectué sur les virus/programmes malveillants probables, mais l'action de scan est configurable.

Spywares et graywares

Les endpoints courent des risques en raison de menaces potentielles autres que des virus/programmes malveillants. Les spywares/graywares sont des applications ou fichiers non classés en tant que virus ou chevaux de Troie, mais qui peuvent toutefois avoir un effet négatif sur les performances des endpoints de votre réseau. Ils font courir un risque significatif à votre entreprise sur le plan de la sécurité et de la confidentialité et peuvent avoir des conséquences judiciaires. Les spywares/graywares réalisent souvent des actions variées non souhaitées et menaçantes, telles que l'affichage de fenêtres pop-up, l'enregistrement des séquences de frappe des touches du clavier et l'exposition des vulnérabilités du endpoint à des attaques.

Si vous découvrez une application ou un fichier qu'OfficeScan ne peut pas détecter comme étant un grayware mais que vous jugez comme en étant un, envoyez-le à Trend Micro pour analyse :

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

TYPE	DESCRIPTION
Spyware	rassemble des données telles que des noms d’utilisateur de comptes et des mots de passe pour les transmettre à des tiers.

Type	Description
Adware	affiche des publicités et rassemble des données telles que les préférences de navigation de l'utilisateur afin de cibler les publicités destinées à cet utilisateur via un navigateur Web.
Numéroteur	Modifie les paramètres Internet du endpoint et peut obliger ce dernier à composer des numéros de téléphone préconfigurés via un modem. Ce sont souvent des numéros de services téléphoniques facturés à l'utilisation (pay-per-call) ou internationaux qui peuvent entraîner une dépense significative pour votre entreprise.
Canular	Entraîne un comportement anormal du endpoint, comme la fermeture et l'ouverture du lecteur de CD-ROM et l'affichage de nombreuses boîtes de message.
Outil de piratage	aide les pirates informatiques à s'infiltrer sur les ordinateurs.
Outil d'accès à distance	aide les pirates informatiques à accéder à distance à plusieurs ordinateurs et à les contrôler.
Application de piratage des mots de passe	aide les pirates informatiques à déchiffrer des noms d'utilisateurs et des mots de passe.
Autres	Autres types de programmes potentiellement malveillants.

Comment les spywares/graywares s'infiltrent-t-ils sur le réseau

Les spywares/graywares s'introduisent généralement dans un réseau d'entreprise lorsque les utilisateurs téléchargent des programmes légitimes dont le module d'installation contient des applications de graywares. La plupart des programmes proposent un contrat de licence utilisateur final (CLUF) que l'utilisateur est tenu d'accepter avant de lancer la procédure de téléchargement. Ce contrat de licence inclut des informations relatives à l'application et à sa fonction de collecte de données personnelles ; toutefois, les utilisateurs négligent souvent ces informations ou ne comprennent pas la terminologie juridique.

Risques et menaces potentiels

La présence de spywares et d'autres types de graywares sur le réseau est susceptible de donner lieu à ce qui suit :

TABLEAU 7-2. Risques et menaces potentiels

RISQUE OU MENACE	DESCRIPTION
Réduction des performances du endpoint	Afin d'exécuter leurs tâches, les applications de spywares/ graywares requièrent souvent une grande partie des ressources du processeur et de la mémoire du système.
Davantage de blocages liés au navigateur Web	Certains types de graywares, tels que les adwares, affichent souvent des informations dans un cadre ou dans la fenêtre du navigateur. Selon le mode d'interaction du code de ces applications avec les processus système, les graywares peuvent parfois provoquer une panne ou un blocage des navigateurs ; un redémarrage du endpoint s'impose parfois.
Diminution de l'efficacité de l'utilisateur	Le fait de devoir fermer fréquemment les fenêtres publicitaires contextuelles et de devoir gérer les effets négatifs des canulars détourne les utilisateurs inutilement de leurs tâches principales.
Dégradation de la bande passante du réseau	Souvent les applications spyware/grayware transmettent régulièrement les données collectées à d'autres applications en cours d'exécution sur le réseau ou à l'extérieur de celui-ci.
Perte d'informations personnelles et de l'entreprise	Les données que les applications de spywares/graywares rassemblent ne sont pas toutes aussi inoffensives qu'une liste de sites Web consultés par les utilisateurs. Le spyware/grayware est également susceptible de recueillir des informations d'identification, comme celles utilisées pour accéder aux comptes bancaires en ligne et aux réseaux d'entreprise.
Risque accru de responsabilité civile	En cas de piratage des ressources du endpoint via le réseau, les pirates peuvent utiliser les ordinateurs des agents pour lancer des attaques ou installer des spywares/graywares sur des ordinateurs situés en dehors du réseau. L'utilisation des ressources du réseau pour des activités de ce genre peut rendre l'entreprise responsable juridiquement des dommages occasionnés aux autres parties.

Protection contre les spywares/graywares et autres menaces

Vous pouvez prendre de nombreuses mesures pour éviter l'installation de spywares/graywares sur votre endpoint. Trend Micro propose d'effectuer les opérations suivantes :

- Configurez tous les types de scans (scan manuel, scan en temps réel, scan programmé et scan immédiat) pour rechercher des fichiers et applications de spywares/graywares et les supprimer. Voir *Types de scan à la page 7-15* pour obtenir plus d'informations.
- Formez les utilisateurs d'agents à effectuer les opérations suivantes :
  - Lire le contrat de licence utilisateur final (CLUF) et la documentation fournie avec les applications téléchargées et installées sur les ordinateurs.
  - Cliquer sur **Non** dans chaque boîte de dialogue demandant l'autorisation de télécharger et d'installer des logiciels, à moins que les utilisateurs des agents ne soient certains que l'auteur du logiciel et le site Web utilisés sont dignes de confiance.
  - Ignorer tout e-mail commercial non sollicité (spam), particulièrement si le spam demande aux utilisateurs de cliquer sur un bouton ou un lien hypertexte.
- Configurez les paramètres du navigateur web afin d'assurer un niveau de sécurité strict. Trend Micro recommande de configurer les navigateurs Web pour qu'ils demandent confirmation aux utilisateurs avant d'installer des contrôles ActiveX.
- Si vous utilisez Microsoft Outlook, configurez les paramètres de sécurité de façon à ce qu'Outlook ne télécharge pas automatiquement des éléments HTML, tels que les images envoyées dans les messages de spam.
- N'autorisez pas l'utilisation de services de partage de fichiers Peer-to-Peer. Les applications de spywares ou autres graywares peuvent se cacher derrière d'autres types de fichiers que les utilisateurs peuvent souhaiter télécharger tels que les fichiers musicaux MP3.
- Examinez régulièrement les logiciels installés sur vos ordinateurs agents et recherchez les applications pouvant être des spywares ou autres graywares.

- Maintenez à jour votre système d'exploitation Windows avec les patchs les plus récents de Microsoft. Consultez le site Web de Microsoft pour plus d'informations.

Types de méthodes de scan

Les agents OfficeScan peuvent utiliser l'une des deux méthodes de scan disponibles pour rechercher des risques de sécurité. Les méthodes de scan sont le Smart Scan et le scan traditionnel.

- **Smart Scan**

  Dans ce document, les agents utilisant Smart Scan sont appelés **agents Smart Scan**. Les agents Smart Scan bénéficient de scans locaux et de requêtes sur le Web fournis par les services File Reputation.

- **Scan traditionnel**

  Les agents n'utilisant pas Smart Scan sont appelés **agents de scan traditionnel**. Un agent de scan traditionnel stocke tous les composants OfficeScan sur le endpoint de l'agent et scanne tous les fichiers localement.

Méthode de scan par défaut

Dans cette version d'OfficeScan, Smart Scan est la méthode de scan par défaut pour les nouvelles installations. En d'autres termes, si vous effectuez une nouvelle installation du serveur OfficeScan sans avoir changé la méthode de scan sur la console Web, tous les agents gérés par le serveur utiliseront Smart Scan.

Si vous mettez à niveau le serveur OfficeScan à partir d'une version antérieure et que la mise à niveau automatique des agents est activée, tous les agents gérés par le serveur utiliseront toujours la méthode de scan configurée avant la mise à niveau. Si vous effectuez une mise à niveau depuis OfficeScan 10, qui prend en charge à la fois Smart Scan et le scan traditionnel, tous les agents ayant été mis à niveau et utilisant Smart Scan continueront de l'utiliser, et tous ceux utilisant le scan traditionnel continueront d'utiliser ce dernier.

Comparaison des méthodes de scan

Le tableau suivant compare les deux méthodes de scan :

Tableau 7-3. Comparaison entre le scan traditionnel et Smart Scan

Base de comparaison	Scan traditionnel	Smart Scan
Disponibilité	Disponible dans cette version d'OfficeScan et toutes les précédentes	Disponible à partir d'OfficeScan 10
Comportement de scan	L'agent de scan traditionnel effectue le scan sur le endpoint local.	• L'agent Smart Scan effectue le scan sur le endpoint local. • S'il ne parvient pas à déterminer le niveau de risque représenté par le fichier durant le scan, il le vérifie en envoyant une requête de scan à une source Smart Protection. • L'agent met en mémoire cache le résultat de la requête de scan afin d'améliorer les performances du scan.
Composants utilisés et mis à jour	Tous les composants disponibles sur la source de mise à jour, hormis Smart Scan Agent Pattern	Tous les composants disponibles sur la source de mise à jour, hormis le fichier de signatures de virus et le celui de surveillance active des spywares
Source de mise à jour habituelle	Serveur OfficeScan	Serveur OfficeScan

Changement de la méthode de scan

Procédure

1. Accédez à **Agents** > **Gestion des agents**.

2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.

3. Cliquez sur **Paramètres** > **Paramètres de scan** > **Méthodes de scan**.

4. Sélectionnez **Scan traditionnel** ou **Smart Scan**.

5. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :

   - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.

   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Passage de Smart Scan au scan traditionnel

Lorsque vous faites passer des agents au scan traditionnel, tenez compte de ce qui suit :

1. **Nombre d'agents à basculer**

   Le basculement simultané d'un nombre d'agents relativement réduit permet d'utiliser efficacement les ressources du serveur OfficeScan , ainsi que celles du serveur Smart Protection Server. Ces serveurs peuvent effectuer d'autres tâches critiques lorsque les agents changent de méthode de scan.

2. **Synchronisation**

   Lorsqu'ils repassent au scan traditionnel, les agents sont susceptibles de télécharger la version complète du fichier de signatures de virus et du fichier de signatures de surveillance active des spywares à partir du serveur OfficeScan . Ces fichiers de signatures ne sont utilisés que par les agents de scan traditionnel.

   Prévoyez d'effectuer le basculement pendant les heures creuses pour vous assurer que le processus de téléchargement se termine rapidement. Prévoyez également

d'effectuer le basculement lorsqu'aucune mise à jour des agents n'est programmée à partir du serveur. De plus, désactivez temporairement l'option « Mettre à jour » sur les agents et réactivez-la lorsque les agents ont basculé vers Smart Scan.

3. **Paramètres de l'arborescence des agents**

   La méthode de scan est un paramètre détaillé qui peut être défini au niveau de la racine, du domaine ou d'un agent individuel. Lorsque vous passez au scan traditionnel, vous pouvez :

   - Créer un nouveau domaine de l'arborescence des agents et définir le scan traditionnel comme sa méthode de scan. Tout agent que vous déplacez vers ce domaine utilisera le scan traditionnel. Lorsque vous déplacez l'agent, activez le paramètre **Appliquer les paramètres du nouveau domaine aux agents sélectionnés**.
   - Sélectionnez un domaine et configurez-le pour utiliser le scan traditionnel. Les agents Smart Scan appartenant au domaine passeront au scan traditionnel.
   - Sélectionnez un ou plusieurs agents Smart Scan dans un domaine et faites-les passer au scan traditionnel.



Remarque

Tout changement de méthode de scan du domaine remplace la méthode que vous avez configurée pour des agents individuels.

Passage du scan traditionnel à Smart Scan

Si vous faites basculer les agents du scan traditionnel vers Smart Scan, assurez-vous d'avoir configuré les Services Smart Protection. Pour obtenir des informations détaillées, voir *Configuration des services Smart Protection à la page 4-13*.

Le tableau suivant donne d'autres éléments à prendre en compte lorsque vous basculez vers le Smart Scan :

TABLEAU 7-4. Éléments à prendre en compte lorsque vous basculez vers Smart Scan

ÉLÉMENTS À PRENDRE EN COMPTE	DÉTAILS
Licence du produit	Pour utiliser Smart Scan, assurez-vous que vous avez activé les licences des services suivants et que ces licences n'ont pas expiré : • Antivirus • Réputation de sites Web et anti-spyware
Serveur OfficeScan	Vérifiez que les agents peuvent se connecter au serveur OfficeScan. Seuls les agents en ligne seront invités à passer à Smart Scan. Les agents hors ligne sont notifiés lorsqu'ils sont en ligne. Les agents itinérants sont notifiés lorsqu'ils sont en ligne ou, dans le cas des agents disposant des privilèges de mise à jour programmée, lors de l'exécution d'une mise à jour programmée. Vérifiez également que le serveur OfficeScan possède les composants les plus récents car les agents Smart Scan doivent télécharger le fichier Smart Scan Agent Pattern à partir du serveur. Pour mettre à jour les composants, reportez-vous à *Mises à jour du serveur OfficeScan à la page 6-17*.
Nombre d'agents à basculer	Le basculement simultané d'un nombre d'agents relativement réduit permet d'utiliser efficacement les ressources du serveur OfficeScan. Le serveur OfficeScan peut effectuer d'autres tâches critiques lorsque les agents changent de méthode de scan.

Éléments à prendre en compte	Détails
Synchronisation	Lorsqu'ils passent à Smart Scan pour la première fois, les agents doivent télécharger la version complète du fichier Smart Scan Agent Pattern à partir du serveur OfficeScan. Le fichier Smart Scan Pattern n'est utilisé que par les agents Smart Scan. Prévoyez d'effectuer le basculement pendant les heures creuses pour vous assurer que le processus de téléchargement se termine rapidement. Prévoyez également d'effectuer le basculement lorsqu'aucune mise à jour des agents n'est programmée à partir du serveur. De plus, désactivez temporairement l'option « Mettre à jour » sur les agents et réactivez-la lorsque les agents ont basculé vers Smart Scan.
Paramètres de l'arborescence des agents	La méthode de scan est un paramètre détaillé qui peut être défini au niveau de la racine, du domaine ou d'un agent individuel. Lorsque vous passez à Smart Scan, vous pouvez: • Créer un nouveau domaine de l'arborescence des agents et définir Smart Scan comme sa méthode de scan. Tout agent que vous déplacez vers ce domaine utilisera Smart Scan. Lorsque vous déplacez l'agent, activez le paramètre **Appliquer les paramètres du nouveau domaine aux agents sélectionnés**. • Sélectionnez un domaine et configurez-le pour utiliser Smart Scan. Les agents de scan traditionnel appartenant au domaine passeront à Smart Scan. • Sélectionnez un ou plusieurs agents de scan traditionnel dans un domaine et faites-les passer à Smart Scan. **Remarque** Tout changement de méthode de scan du domaine remplace la méthode que vous avez configurée pour des agents individuels.

Éléments à prendre en compte	Détails
Prise en charge d'IPv6	Les agents Smart Scan envoient des requêtes de scan aux sources Smart Protection. Un agent Smart Scan IPv6 pur ne peut pas envoyer directement de requêtes à des sources IPv4 pures, telles que : • Smart Protection Server 2.0 (intégré ou autonome) **Remarque** IPv6 est pris en charge pour le serveur Smart Protection Server à partir de la version 2.5. • Trend Micro Smart Protection Network De même, un agent Smart Scan IPv4 pur ne peut pas envoyer de requêtes à des serveurs Smart Protection IPv6 purs. Un serveur proxy à double pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre aux agents Smart Scan de se connecter aux sources.

Types de scan

OfficeScan propose les types de scan suivants afin de protéger les ordinateurs des agents OfficeScan contre les risques de sécurité :

Tableau 7-5. Types de scan

Type de scan	Description
Scan en temps réel	Désigne un scan automatique d'un fichier sur le endpoint dès sa réception, son ouverture, son téléchargement, sa copie ou sa modification Voir *Scan en temps réel à la page 7-16* pour obtenir des informations détaillées.

TYPE DE SCAN	DESCRIPTION
Scan manuel	désigne un scan initié par l'utilisateur qui analyse un fichier ou un ensemble de fichiers à la demande de ce dernier. Voir *Scan manuel à la page 7-19* pour obtenir des informations détaillées.
Scan programmé	Désigne un scan automatique des fichiers du endpoint selon la programmation configurée par l'administrateur ou par l'utilisateur Voir *Scan programmé à la page 7-21* pour obtenir des informations détaillées.
Scan immédiat	Désigne un scan lancé par l'administrateur qui scanne les fichiers sur un ou plusieurs ordinateurs cibles Voir *Scan immédiat à la page 7-24* pour obtenir des informations détaillées.

Scan en temps réel

Le scan en temps réel s'effectue en continu. Lors de la réception, de l'ouverture, du téléchargement, de la copie ou de la modification d'un fichier, le scan en temps réel recherche les risques pour la sécurité. Si OfficeScan ne détecte aucun risque de sécurité, le fichier demeure à sa place et les utilisateurs peuvent y accéder. Si un risque de sécurité ou un programme malveillant probable est détecté, OfficeScan affiche un message de notification avec le nom du fichier infecté et le risque spécifique lié à la sécurité.

Le scan en temps réel dispose d'une mémoire cache persistante rechargée à chaque démarrage de l'agent OfficeScan. Si des fichiers ou des dossiers ont été modifiés depuis le dernier déchargement de l'agent OfficeScan, ce dernier les supprime de la mémoire cache.



Remarque

Pour modifier le message de notification, ouvrez la console Web et accédez à **Administration** > **Notification** > **Agent**.

Configurez et appliquez des paramètres de scan en temps réel à un ou plusieurs agents et domaines, ou à tous les agents gérés par le serveur.

Configuration des paramètres de scan en temps réel

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Paramètres de scan** > **Paramètres de scan en temps réel**.
4. Sélectionnez les options suivantes :
   - Activer le scan antivirus/programme malveillant
   - Activer le scan antispyware/grayware

   Remarque

   Si vous désactivez le scan antivirus/programmes malveillants, le scan anti-spywares/graywares se désactive également. Au cours d'une épidémie virale, le scan en temps réel ne peut pas être désactivé (ou sera activé automatiquement s'il était désactivé au départ) pour empêcher les virus de modifier ou de supprimer les fichiers et les dossiers sur les ordinateurs des agents.

5. Configurez les critères suivants pour le scan :
   - *Action des utilisateurs sur les fichiers à la page 7-28*
   - *Fichiers à scanner à la page 7-29*
   - *Paramètres de scan à la page 7-29*
   - *Exclusions de scan à la page 7-33*
6. Cliquez sur l'onglet **Action**, puis configurez ce qui suit :

TABLEAU 7-6. Actions du scan en temps réel

ACTION	RÉFÉRENCE
Action des virus/ programmes malveillants	Action principale (en sélectionner une) : • *Utiliser ActiveAction à la page 7-39* • *Utilisez la même action pour tous les types de virus/ programmes malveillants à la page 7-41* • *Utilisez une action spécifique pour chaque type de virus/programme malveillant à la page 7-41* **Remarque** Pour plus de détails sur les différentes actions, reportez-vous à *Actions de scan antivirus/ programmes malveillants à la page 7-38*. Actions de virus/programmes malveillants supplémentaires : • *Répertoire de quarantaine à la page 7-42* • *Sauvegardez les fichiers avant nettoyage à la page 7-44* • *Damage Cleanup Services à la page 7-44* • *Afficher un message de notification lorsqu'un virus/ programme malveillant est détecté à la page 7-45* • *Afficher un message de notification lorsqu'un virus/ programme malveillant potentiel est détecté à la page 7-46*
Action de spywares/ graywares	Action principale : • *Actions de scan anti-spywares/graywares à la page 7-51* Action de spywares/graywares supplémentaires : • *Afficher un message de notification lorsqu'un spyware/grayware est détecté à la page 7-52*

7. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :

    - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.

    - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Scan manuel

Le scan manuel est un scan à la demande qui démarre immédiatement après avoir été lancé par un utilisateur depuis la console de l'agent OfficeScan. La durée du scan dépend du nombre de fichiers spécifiés pour le scan et des ressources matérielles du endpoint de l'agent OfficeScan.

Configurez et appliquez des paramètres de scan manuel à un ou plusieurs agents et domaines, ou à tous les agents gérés par le serveur.

Configuration d'un scan manuel

Procédure

1. Accédez à **Agents** > **Gestion des agents**.

2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.

3. Cliquez sur **Paramètres** > **Paramètres de scan** > **Paramètres de scan manuel**.

4. Dans l'onglet **Cible**, configurez ce qui suit :

    - *Fichiers à scanner à la page 7-29*

- *Paramètres de scan à la page 7-29*
- *Utilisation de l'processeur à la page 7-31*
- *Exclusions de scan à la page 7-33*

5. Cliquez sur l'onglet **Action**, puis configurez ce qui suit :

TABLEAU 7-7. Actions du scan manuel

ACTION	RÉFÉRENCE
Action des virus/ programmes malveillants	Action principale (en sélectionner une) : • *Utiliser ActiveAction à la page 7-39* • *Utilisez la même action pour tous les types de virus/ programmes malveillants à la page 7-41* • *Utilisez une action spécifique pour chaque type de virus/programme malveillant à la page 7-41* **Remarque** Pour plus de détails sur les différentes actions, reportez-vous à *Actions de scan antivirus/ programmes malveillants à la page 7-38*. Actions de virus/programmes malveillants supplémentaires : • *Répertoire de quarantaine à la page 7-42* • *Sauvegardez les fichiers avant nettoyage à la page 7-44* • *Damage Cleanup Services à la page 7-44*
Action de spywares/ graywares	Action principale : • *Actions de scan anti-spywares/graywares à la page 7-51*

6. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :

- **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.
- **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Scan programmé

Un scan programmé démarre automatiquement aux date et heure programmées. Utilisez le scan programmé pour automatiser les scans de routine sur l'agent et améliorer l'efficacité de votre gestion des scans.

Configurez et appliquez des paramètres de scan programmé à un ou plusieurs agents et domaines, ou à tous les agents gérés par le serveur.

Configuration d'un scan programmé

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Paramètres de scan** > **Paramètres de scan programmé**.
4. Sélectionnez les options suivantes :
    - **Activer le scan antivirus/programme malveillant**
    - **Activer le scan antispyware/grayware**



Remarque

Si vous désactivez le scan antivirus/programmes malveillants, le scan anti-spywares/graywares se désactive également.

5. Configurez les critères suivants pour le scan :

- *Programmation à la page 7-32*
- *Fichiers à scanner à la page 7-29*
- *Paramètres de scan à la page 7-29*
- *Utilisation de l'processeur à la page 7-31*
- *Exclusions de scan à la page 7-33*

6. Cliquez sur l'onglet **Action**, puis configurez ce qui suit :

TABLEAU 7-8. Actions de scan programmé

ACTION	RÉFÉRENCE
Action des virus/ programmes malveillants	Action principale (en sélectionner une) : • *Utiliser ActiveAction à la page 7-39* • *Utilisez la même action pour tous les types de virus/ programmes malveillants à la page 7-41* • *Utilisez une action spécifique pour chaque type de virus/programme malveillant à la page 7-41* **Remarque** Pour plus de détails sur les différentes actions, reportez-vous à *Actions de scan antivirus/ programmes malveillants à la page 7-38*. Actions de virus/programmes malveillants supplémentaires : • *Répertoire de quarantaine à la page 7-42* • *Sauvegardez les fichiers avant nettoyage à la page 7-44* • *Damage Cleanup Services à la page 7-44* • *Afficher un message de notification lorsqu'un virus/ programme malveillant est détecté à la page 7-45* • *Afficher un message de notification lorsqu'un virus/ programme malveillant potentiel est détecté à la page 7-46*
Action de spywares/ graywares	Action principale : • *Actions de scan anti-spywares/graywares à la page 7-51* Action de spywares/graywares supplémentaires : • *Afficher un message de notification lorsqu'un spyware/grayware est détecté à la page 7-52*

7. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :

    - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.

    - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Scan immédiat

Le scan immédiat est lancé à distance par un administrateur OfficeScan via la console Web et peut concerner un ou plusieurs ordinateurs des agents.

Configurez et appliquez des paramètres de scan immédiat à un ou plusieurs agents et domaines, ou à tous les agents gérés par le serveur.

Configuration des paramètres de scan immédiat

Procédure

1. Accédez à **Agents** > **Gestion des agents**.

2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.

3. Cliquez sur **Paramètres** > **Paramètres de scan** > **Paramètres de scan immédiat**.

4. Sélectionnez les options suivantes :

    - **Activer le scan antivirus/programme malveillant**

    - **Activer le scan antispyware/grayware**



Remarque

Si vous désactivez le scan antivirus/programmes malveillants, le scan anti-spywares/ graywares se désactive également.

5. Configurez les critères suivants pour le scan :

    - *Fichiers à scanner à la page 7-29*
    - *Paramètres de scan à la page 7-29*
    - *Utilisation de l'processeur à la page 7-31*
    - *Exclusions de scan à la page 7-33*

6. Cliquez sur l'onglet **Action**, puis configurez ce qui suit :

TABLEAU 7-9. Actions de scan immédiat

ACTION	RÉFÉRENCE
Action des virus/ programmes malveillants	Action principale (en sélectionner une) : • *Utiliser ActiveAction à la page 7-39* • *Utilisez la même action pour tous les types de virus/ programmes malveillants à la page 7-41* • *Utilisez une action spécifique pour chaque type de virus/programme malveillant à la page 7-41* **Remarque** Pour plus de détails sur les différentes actions, reportez-vous à *Actions de scan antivirus/ programmes malveillants à la page 7-38*. Actions de virus/programmes malveillants supplémentaires : • *Répertoire de quarantaine à la page 7-42* • *Sauvegardez les fichiers avant nettoyage à la page 7-44* • *Damage Cleanup Services à la page 7-44*

ACTION	RÉFÉRENCE
Action de spywares/ graywares	Action principale : • *Actions de scan anti-spywares/graywares à la page 7-51*

7. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :

   - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.

   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Exécution du scan immédiat

Lancez un Scan immédiat sur les ordinateurs susceptibles d'être infectés.

Procédure

1. Accédez à **Agents** > **Gestion des agents**.

2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.

3. Cliquez sur **Tâches** > **Scan immédiat**.

4. Pour modifier les paramètres de **scan immédiat** préconfigurés avant le lancement du scan, cliquez sur **Paramètres**.

   L'écran **Paramètres de scan immédiat** s'affiche. Voir *Scan immédiat à la page 7-24* pour obtenir des informations détaillées.

5. Dans l'arborescence des agents, sélectionnez les agents devant exécuter un scan et cliquez sur **Lancer un scan immédiat**.



Remarque

Si vous ne sélectionnez aucun agent, OfficeScan envoie automatiquement une notification à tous les agents de l'arborescence des agents.

Le serveur envoie une notification aux agents.

6. Vérifiez l'état de notification et assurez-vous que tous les agents ont reçu une notification.

7. Cliquez sur **Sélectionner les endpoints n'ayant pas reçu de notification**, puis sur **Lancer un scan immédiat** pour envoyer immédiatement une nouvelle notification aux agents ne l'ayant pas encore reçu.

   Exemple : Nombre total d'agents : 50

   Tableau 7-10. Scénarios concernant les agents n'ayant pas reçu de notification

Sélection dans l'arborescence des agents	Agents ayant reçu une notification (après sélection de l'option « Lancer un scan immédiat »)	Agents n'ayant pas reçu de notification
Aucun (la totalité des 50 agents est sélectionnée automatiquement)	35 agents sur 50	15 agents
Sélection manuelle (45 agents sur 50 sélectionnés)	40 agents sur 45	5 agents + 5 autres agents non inclus dans la sélection manuelle

8. Cliquez sur **Arrêter la notification** pour qu'OfficeScan arrête d'envoyer des notifications aux agents recevant actuellement des notifications. Les agents ayant déjà reçu la notification et dont le processus de scan est en cours ignorent cette commande.

9. Pour les agents dont le processus de scan a commencé, cliquez sur **Arrêter le scan immédiat** pour leur demander d'arrêter le scan.

Paramètres communs à tous les types de scan

Pour chaque type de scan, configurez trois ensembles de paramètres : Critères de scan, exclusions de scan et actions de scan. Déployez ces paramètres sur un ou plusieurs agents et domaines, ou sur tous les agents gérés par le serveur.

Critères de scan

Spécifiez les fichiers qu'un type de scan donné doit scanner en utilisant des attributs de fichier tels que le type de fichier et l'extension. Spécifiez également les conditions qui déclencheront le scan. Par exemple, configurez le scan en temps réel pour scanner chaque fichier après son téléchargement sur le endpoint.

Action des utilisateurs sur les fichiers

Choisissez les actions sur les fichiers qui déclenchent le scan en temps réel. Sélectionnez l'une des options suivantes :

- **Scanner les fichiers en cours de création/modification** : scanne les nouveaux fichiers ajoutés au endpoint (par exemple, après leur téléchargement) ou les fichiers en cours de modification
- **Scanner les fichiers en cours de récupération** : scanne les fichiers lorsqu'ils sont ouverts
- **Scanner les fichiers en cours de création/modification et de récupération**

Par exemple, si la troisième option est sélectionnée, un nouveau fichier téléchargé sur le endpoint est scanné et reste à son emplacement actuel si aucun risque de sécurité n'est détecté. Le même fichier est scanné lorsqu'un utilisateur l'ouvre et, s'il a modifié ce fichier, avant l'enregistrement des modifications.

Fichiers à scanner

Sélectionnez l'une des options suivantes :

- **Tous les fichiers scannables** : Scanner tous les fichiers
- **Types de fichiers scannés par IntelliScan** : scanne uniquement les fichiers connus pour contenir potentiellement du code malveillant, y compris ceux dissimulés sous une extension inoffensive. Voir *IntelliScan à la page E-6* pour obtenir des informations détaillées.
- **Fichiers portant les extensions suivantes** : scanne uniquement les fichiers dont les extensions figurent dans la liste des extensions de fichier. Ajoutez de nouvelles extensions ou supprimez des extensions existantes.

Paramètres de scan

Sélectionnez une ou plusieurs des options suivantes :

- **Scanner la disquette pendant l'arrêt du système** : le scan en temps réel scanne les disquettes à la recherche de virus d'amorce avant l'arrêt du endpoint. Cela évite que des virus/programmes malveillants ne s'exécutent lorsqu'un utilisateur redémarre le endpoint à partir de la disquette.
- **Scanner les dossiers masqués** : permet à OfficeScan de détecter puis de scanner les dossiers masqués sur le endpoint au cours d'un scan manuel.
- **Scanner les lecteurs de réseau** : scanne les lecteurs ou les dossiers réseau mappés sur le endpoint de l'agent OfficeScan au cours du scan manuel ou du scan en temps réel.
- **Scanner le secteur d'amorçage du périphérique de stockage USB après sa connexion** : scanne automatiquement uniquement le secteur d'amorçage d'un périphérique de stockage USB à chaque fois que l'utilisateur le connecte (scan en temps réel).
- **Scanner tous les fichiers des périphériques de stockage amovibles lors de leur connexion** : Scanne automatiquement tous les fichiers d'un périphérique de stockage USB à chaque fois que l'utilisateur le connecte (scan en temps réel).
- **Des variantes de programmes malveillants en quarantaine sont détectées dans la mémoire** : La surveillance des comportements scanne la mémoire du

système à la recherche de processus suspects ; le scan en temps réel mappe le processus et le scanne, à la recherche de menaces liées à des programmes malveillants. Si une menace liée à un programme malveillant existe, le scan en temps réel met le processus et/ou le fichier en quarantaine.



Remarque

Cette fonctionnalité requiert l'activation par les administrateurs du service de prévention des modifications non autorisées et du service de protection avancé.

- **Scanner les fichiers compressés** : permet à OfficeScan de scanner un nombre maximum spécifié de couches de compression et de ne pas scanner les couches supplémentaires. OfficeScan nettoie aussi ou supprime les fichiers infectés dans les fichiers compressés. Par exemple, si le maximum que vous avez choisi est de deux couches et qu'un fichier à scanner comprend six couches, OfficeScan analyse deux couches sans analyser les quatre suivantes. Si un fichier compressé contient des risques de sécurité, OfficeScan le nettoie ou le supprime.



Remarque

OfficeScan traite les fichiers Microsoft Office 2007 au format Office Open XML comme étant des fichiers compressés. Office Open XML, format de fichier des applications Office 2007, utilise les technologies de compression ZIP. Si vous voulez que les fichiers créés à l'aide de ces applications soient scannés pour détecter les virus/programmes malveillants, vous devez activer le scan des fichiers compressés.

- **Scanner les objets OLE** : Lorsqu'un fichier contient plusieurs couches Object Linking and Embedding (OLE), OfficeScan analyse le nombre de couches que vous spécifiez et ignore les autres.

  Tous les agents OfficeScan gérés par le serveur vérifient ce paramètre lors du scan manuel, du scan en temps réel, du scan programmé et du scan immédiat. Chaque couche fait l'objet d'un scan antivirus/programme malveillant et antispyware/grayware.

  Par exemple :

  Le nombre de couches que vous spécifiez est de 2. Un fichier intègre un document Microsoft Word (première couche), qui comporte une feuille de calcul Microsoft Excel (deuxième couche), qui contient un fichier `.exe` (troisième couche).

OfficeScan scanne le document Word et la feuille de calcul Excel et ignore le fichier `.exe`.

- **Détecter le code d'exploitation dans les fichiers OLE** : La détection d'exploitation OLE identifie les programmes malveillants de manière heuristique en vérifiant la présence de code d'exploitation dans les fichiers Microsoft Office.



Remarque

Le nombre spécifié de couches s'applique à la fois aux options **Scanner les objets OLE** et **Détecter le code d'exploitation**.

- **Activer IntelliTrap** : détecte et supprime les virus/programmes malveillants des fichiers exécutables compressés. Cette option est uniquement disponible pour le scan en temps réel. Voir *IntelliTrap à la page E-7* pour obtenir des informations détaillées.

- **Scanner la zone d'amorçage** : recherche des virus/programmes malveillants dans le secteur d'amorçage du disque dur du endpoint de l'agent lors du scan manuel, du scan programmé et du scan immédiat.

Utilisation de l'processeur

OfficeScan peut s'interrompre entre le scan d'un fichier et le scan du suivant. Ce paramètre est utilisé lors du scan manuel, du scan programmé et du scan immédiat.

Sélectionnez l'une des options suivantes :

- **Élevé** : aucune interruption entre les scans
- **Moyen** : interruption entre les scans de fichiers si la consommation de l'processeur est supérieure à 50% et pas d'interruption si elle est de 50% ou moins
- **Faible** : interruption entre les scans de fichiers si la consommation de l'processeur est supérieure à 20% et pas d'interruption si elle est de 20% ou moins

Si vous choisissez Moyen ou Faible, lorsque le scan démarre et si la consommation de l'processeur respecte le seuil (50% ou 20%), OfficeScan ne s'interrompt pas entre les scans, ce qui se traduit par des temps de scan plus rapides. OfficeScan utilise plus de

ressources de l'processeur au cours du processus, mais du fait que la consommation de l'processeur est optimale, les performances du endpoint ne sont pas affectées de façon significative. Lorsque la consommation de l'processeur commence à dépasser le seuil, OfficeScan s'interrompt pour réduire l'utilisation de l'processeur, et reprend lorsque la consommation revient sous le seuil indiqué.

Si vous choisissez Élevé, OfficeScan ne vérifie pas la consommation réelle de l'processeur et scanne les fichiers sans interruption.

Programmation

Configurez la fréquence (quotidienne, hebdomadaire ou mensuelle) et l'heure à laquelle le scan programmé démarre.

Pour les scans programmés mensuellement, vous pouvez choisir un jour particulier d'un mois ou un jour de la semaine ainsi que l'ordre de son occurrence.

- **Un jour particulier d'un mois** : Sélectionnez un jour entre le 1er et le 31. Si vous avez sélectionnez le 29, le 30 ou le 31 et si un mois ne comporte pas ce jour, OfficeScan exécute le scan programmé le dernier jour du mois. Par conséquent :
  - Si vous avez sélectionné 29, le scan programmé s'exécute le 28 février (sauf en cas d'année bissextile) et le 29e jour de tous les autres mois.
  - Si vous avez sélectionné 30, le scan programmé s'exécute le 28 ou le 29 février et le 30ème jour de tous les autres mois.
  - Si vous avez sélectionné 31, le scan programmé s'exécute le 28 ou le 29 février, le 30 avril, le 30 juin, le 30 septembre, le 30 novembre et le 31ème jour de tous les autres mois.
- **Un jour de la semaine et l'ordre de son occurrence** : Un jour de la semaine se produit quatre ou cinq fois par mois. Par exemple, il y a généralement quatre lundis chaque mois. Indiquez un jour de la semaine et l'ordre dans lequel il se produit au cours d'un mois. Par exemple, choisissez d'exécuter le scan programmé le second lundi de chaque mois. Si vous choisissez la cinquième occurrence d'un jour de la semaine, et si ce jour n'existe pas au cours d'un mois donné, le scan s'exécute à la quatrième occurrence.

Exclusions de scan

Configurez des exclusions de scan afin d'améliorer les performances du scan et d'ignorer les fichiers provoquant de fausses alertes. Lorsqu'un type de scan particulier s'exécute, OfficeScan examine la liste des exclusions de scan pour déterminer les fichiers du endpoint qui seront exclus de la recherche de virus/programmes malveillants et de spywares/graywares.

Lorsque vous activez des exclusions de scan, OfficeScan ne scanne pas un fichier dans les conditions suivantes :

- Le fichier se trouve dans un répertoire donné (ou dans l'un de ses sous-répertoires).
- Le nom du fichier correspond à l'un de ceux de la liste d'exclusion.
- L'extension du fichier correspond à l'une de celles de la liste d'exclusion.



Conseil

Pour obtenir une liste de produits que Trend Micro recommande d'exclure des scans en temps réel, accédez à :

http://esupport.trendmicro.com/solution/en-US/1059770.aspx

Exceptions avec caractères génériques

Les listes d'exclusion de scan pour les fichiers et les répertoires prennent en charge l'utilisation des caractères génériques. Utilisez le caractère « ? » pour remplacer un caractère et « * » pour en remplacer plusieurs.

Utilisez les caractères génériques avec précaution. L'utilisation d'un caractère erroné peut exclure des fichiers ou des répertoires incorrects. Par exemple, l'ajout de `C:\*` à la liste des exclusions de scan (fichiers) exclut l'intégralité du lecteur `C:\`.

TABLEAU 7-11. Exclusions de scan avec des caractères génériques

VALEUR	EXCLUS	NON EXCLUS

`c:\director*\fil\*.txt`	`c:\directory\fil\doc.txt`
	`c:\directories\fil\files\document.txt`
		`c:\directory\file\`
		`c:\directories\files\`
		`c:\directory\file\doc.txt`
		`c:\directories\files\document.txt`

`c:\director?\file\*.txt`	`c:\directory\file\doc.txt`	`c:\directories\file\document.txt`
`c:\director?\file\?.txt`	`c:\directory\file\1.txt`	`c:\directory\file\doc.txt` `c:\directories\file\document.txt`
`c:\*.txt`	Tous les fichiers `.txt` du répertoire `C:\`	Tous les autres types de fichiers du répertoire `C:\`
`[]`	Non pris en charge	Non pris en charge
`*.*`	Non pris en charge	Non pris en charge

Liste d'exclusion de scan (répertoires)

OfficeScan ne scanne pas l'ensemble des fichiers contenus dans un répertoire spécifique de l'ordinateur. Vous pouvez spécifier au maximum 256 répertoires.



Remarque

Une fois qu'un répertoire donné est exclu des actions de scans, OfficeScan exclut également automatiquement l'ensemble des sous-répertoires de ce répertoire.

Vous pouvez également choisir l'option **Exclure les répertoires dans lesquels sont installés des produits Trend Micro**. Si vous sélectionnez cette option, OfficeScan exclut automatiquement du scan les répertoires des produits Trend Micro suivants :

- <*Dossier d'installation du serveur*>

- ScanMail™ for Microsoft Exchange (toutes les versions sauf la version 7). Si vous utilisez la version 7, ajoutez les dossiers suivants à la liste des exclusions :
  - `\Smex\Temp`
  - `\Smex\Storage`
  - `\Smex\ShareResPool`
- ScanMail eManager™ 3.11, 5.1, 5.11 et 5.12
- ScanMail for Lotus Notes™ eManager NT
- InterScan Web Security Suite
- InterScan Web Protect
- InterScan FTP VirusWall
- InterScan Web VirusWall
- InterScan E-mail VirusWall
- InterScan VirusWall 3.53
- InterScan NSAPI Plug-in
- InterScan eManager 3.5x

Si vous disposez d'un produit Trend Micro NON répertorié dans la liste, ajoutez manuellement les répertoires de ce produit à la liste d'exclusion de scan.

Configurez également OfficeScan pour exclure les répertoires Microsoft Exchange 2000/2003 en accédant à la section **Paramètres de scan** sous **Agents** > **Paramètres de l'agent général**. Si vous utilisez Microsoft Exchange 2007 ou une version plus récente, ajoutez manuellement le répertoire à la liste d'exclusion de scan. Reportez-vous au site suivant pour obtenir des informations détaillées sur les exclusions de scan :

http://technet.microsoft.com/en-us/library/bb332342.aspx

Lorsque vous configurez la liste de fichiers, choisissez l'une des options suivantes :

- **Conservation de la liste actuelle** (valeur par défaut) : cette option est proposée par OfficeScan pour empêcher l'écrasement involontaire de la liste des exclusions

existante d'un agent. Pour enregistrer et déployer les modifications apportées à la liste des exclusions, sélectionnez l'une des autres options.

- **Écrasement des données** : cette option supprime l'intégralité de la liste des exclusions de l'agent et la remplace par la liste actuelle. Lorsque vous cliquez sur **Appliquer à tous les agents**, OfficeScan affiche un message de confirmation.
- **Ajout des chemins d'accès à** : cette option ajoute les éléments de la liste actuelle à la liste des exclusions existante de l'agent. Si un élément existe déjà dans la liste des exclusions de l'agent, cet élément est ignoré.
- **Suppression des chemins d'accès de** : cette option supprime les éléments de la liste actuelle de la liste des exclusions existante de l'agent (s'ils y sont présents).

Liste d'exclusion de scan (fichiers)

OfficeScan ne scanne pas un fichier si son nom correspond à l'un de ceux de la liste d'exclusion. Si vous souhaitez exclure un fichier qui se trouve à un emplacement spécifique du endpoint, indiquez son chemin d'accès, par exemple `C:\Temp\sample.jpg`.

Vous pouvez spécifier au maximum 256 fichiers.

Lorsque vous configurez la liste de fichiers, choisissez l'une des options suivantes :

- **Conservation de la liste actuelle** (valeur par défaut) : cette option est proposée par OfficeScan pour empêcher l'écrasement involontaire de la liste des exclusions existante d'un agent. Pour enregistrer et déployer les modifications apportées à la liste des exclusions, sélectionnez l'une des autres options.
- **Écrasement des données** : cette option supprime l'intégralité de la liste des exclusions de l'agent et la remplace par la liste actuelle. Lorsque vous cliquez sur **Appliquer à tous les agents**, OfficeScan affiche un message de confirmation.
- **Ajout des chemins d'accès à** : cette option ajoute les éléments de la liste actuelle à la liste des exclusions existante de l'agent. Si un élément existe déjà dans la liste des exclusions de l'agent, cet élément est ignoré.
- **Suppression des chemins d'accès de** : cette option supprime les éléments de la liste actuelle de la liste des exclusions existante de l'agent (s'ils y sont présents).

Liste d'exclusion de scan (extensions de fichier)

OfficeScan ne scanne pas un fichier si son extension correspond à l'une de celles de la liste d'exclusion. Vous pouvez spécifier au maximum 256 extensions de fichier. Le point (.) n'est pas nécessaire devant l'extension.

Pour le scan en temps réel, utilisez un astérisque (*) comme caractère générique lorsque vous spécifiez des extensions. Par exemple, si vous ne souhaitez pas scanner tous les fichiers dont les extensions commencent par D, comme `DOC`, `DOT` ou `DAT`, saisissez `D*`.

Pour le scan manuel, le scan programmé et le scan immédiat, utilisez un point d'interrogation (?) ou un astérisque (*) comme caractère générique.

Appliquer les paramètres d'exclusion à tous les types de scan

OfficeScan permet de configurer les paramètres d'exclusion pour un type de scan particulier, puis d'appliquer ces mêmes paramètres à tous les autres types de scan. Par exemple :

Le 1er janvier, Chris, administrateur OfficeScan, a découvert qu'il existait un grand nombre de fichiers `JPG` sur les ordinateurs des agents et que ces fichiers ne présentaient pas de menaces de sécurité. Chris a ajouté `JPG` à la liste d'exclusion de fichiers pour le scan manuel et appliqué ce paramètre à tous les types de scan. Le scan en temps réel, le scan immédiat et le scan programmé sont maintenant configurés pour ignorer le scan des fichiers `.jpg`.

Une semaine plus tard, Chris a retiré `JPG` de la liste d'exclusion pour le scan en temps réel mais n'a pas appliqué les paramètres d'exclusions à tous les types de scan. Les fichiers `JPG` seront désormais scannés mais seulement lors du scan en temps réel.

Actions de scan

Spécifiez l'action qu'OfficeScan effectue lorsqu'un type de scan particulier détecte un risque de sécurité. OfficeScan dispose d'un ensemble d'actions de scan différent pour les virus/programmes malveillants et les spywares/graywares.

Actions de scan antivirus/programmes malveillants

L'action de scan entreprise par OfficeScan dépend du type de virus/programme malveillant et du type de scan qui a détecté le virus/programme malveillant. Par exemple, lorsqu'OfficeScan détecte un cheval de Troie (virus/programme malveillant) lors du scan manuel (type de scan), il nettoie (action) le fichier infecté.

Pour plus d'informations sur les différents types de virus/programmes malveillants, reportez-vous à *Virus et programmes malveillants à la page 7-2*

Voici la liste des actions qu'OfficeScan peut effectuer pour lutter contre les virus/ programmes malveillants :

Tableau 7-12. Actions de scan antivirus/programmes malveillants

Action	Description
Supprimer	OfficeScan supprime le fichier infecté.
Quarantaine	OfficeScan renomme puis déplace le fichier infecté vers un répertoire de quarantaine temporaire sur le endpoint de l'agent dans le répertoire <*dossier d'installation de l'agent*>`\Suspect`. L'agent OfficeScan envoie ensuite les fichiers mis en quarantaine vers le répertoire de quarantaine désigné. Voir *Répertoire de quarantaine à la page 7-42* pour obtenir des informations détaillées. Le répertoire de quarantaine par défaut se trouve sur le serveur OfficeScan, sous <*fichier d'installation du serveur*>`\PCCSRV\Virus`. OfficeScan chiffre les fichiers en quarantaine envoyés à ce répertoire. Si vous devez restaurer un fichier mis en quarantaine, utilisez l'outil VSEncrypt. Pour plus d'informations sur l'utilisation de cet outil, consultez *Server Tuner à la page 13-58*.

ACTION	DESCRIPTION
Nettoyer	OfficeScan nettoie le fichier infecté avant d'autoriser l'accès complet au fichier. Si le fichier n'est pas nettoyable, OfficeScan effectue une seconde action qui peut être l'une des actions suivantes : Mettre en quarantaine, Supprimer, Renommer et Ignorer. Pour configurer la deuxième action, accédez à **Agents** > **Gestion des agents**. Cliquez sur l'onglet **Paramètres** > **Paramètres de scan** > **{Type de scan}** > **Action**. Cette action peut effectuée sur tous les types de programmes malveillants, à l'exception des virus/programmes malveillants probables.
Renommer	OfficeScan remplace l'extension du fichier infecté par « `vir` ». Initialement, les utilisateurs ne peuvent pas ouvrir le fichier renommé. Ils peuvent l'ouvrir s'ils associent le fichier à une application déterminée. Le virus/programme malveillant peut s'exécuter lors de l'ouverture du fichier infecté renommé.
Ignorer	OfficeScan ne peut utiliser cette action de scan que lorsqu'il détecte un type de virus donné, lors du scan manuel, du scan programmé et du scan immédiat. OfficeScan ne peut pas utiliser cette action de scan lors du scan en temps réel car l'absence d'action lorsque une tentative d'ouverture ou d'exécution d'un fichier infecté est détectée permettra au virus/programme malveillant de s'exécuter. Toutes les autres actions de scan peuvent être utilisées lors du scan en temps réel.
Refuser l'accès	Cette action de scan ne peut être effectuée que pendant un scan en temps réel. Lorsqu'OfficeScan détecte une tentative d'ouverture ou d'exécution d'un fichier infecté, il bloque immédiatement l'opération. Les utilisateurs peuvent supprimer manuellement le fichier infecté.

Utiliser ActiveAction

À chaque type de virus/programme malveillant correspond une action de scan différente. Pour personnaliser une action de scan, vous devez avoir les connaissances nécessaires sur les virus et programmes malveillants. Cette tâche peut s'avérer fastidieuse. OfficeScan utilise ActiveAction pour pallier à ces problèmes.

ActiveAction est un ensemble d'actions de scan pré-configurées, destinées à lutter contre les virus et les programmes malveillants. Si les actions de scan ne vous sont pas

familières ou si vous ignorez quelle action est la mieux adaptée à tel ou tel type de virus ou programme malveillant, l'utilisation de l'outil ActiveAction est recommandée.

ActiveAction offre les avantages suivants :

- ActiveAction applique les actions de scan recommandées par Trend Micro. Vous ne perdez plus votre temps à configurer vous-même les actions de scan.
- Les créateurs de virus et programmes malveillants modifient en permanence la manière dont leurs virus attaquent les ordinateurs. Les paramètres d'ActiveAction sont mis à jour pour assurer une protection contre les menaces et les méthodes d'attaques les plus récentes des virus et programmes malveillants.



Remarque

ActiveAction n'est pas disponible pour le scan anti-spywares/graywares.

Le tableau suivant illustre comment ActiveAction traite chaque type de virus/programme malveillant :

Tableau 7-13. Actions de scan recommandées par Trend Micro contre les virus et les programmes malveillants

Type de virus/programmes malveillants	Scan en temps réel		Scan manuel/Scan programmé/Scan immédiat	
	Première action	Deuxième action	Première action	Deuxième action
Canular	Quarantaine	Supprimer	Quarantaine	Supprimer
cheval de Troie	Quarantaine	Supprimer	Quarantaine	Supprimer
Virus	Nettoyer	Quarantaine	Nettoyer	Quarantaine
Virus de test	Refuser l'accès	N/A	Ignorer	N/A
Utilitaire de compression	Quarantaine	N/A	Quarantaine	N/A
Autres	Nettoyer	Quarantaine	Nettoyer	Quarantaine

Type de virus/ programmes malveillants	Scan en temps réel		Scan manuel/Scan programmé/ Scan immédiat	
	Première action	Deuxième action	Première action	Deuxième action
Virus/programmes malveillants probables	Refuser l'accès ou action configurée par l'utilisateur	N/A	Ignorer ou action configurée par l'utilisateur	N/A

Pour les virus et programmes malveillants potentiels, l'action par défaut est « Refuser l'accès » pendant le scan en temps réel et « Ignorer » pendant le scan manuel, le scan programmé et le scan immédiat. S'il ne s'agit pas des actions que vous souhaitez effectuer, vous pouvez les modifier par Mettre en quarantaine, Supprimer ou Renommer.

Utilisez la même action pour tous les types de virus/ programmes malveillants

Sélectionnez cette option si vous souhaitez que la même action soit entreprise sur tous les types de virus/programmes malveillants, à l'exception de ceux qui sont potentiels. Si vous choisissez «Nettoyer» comme première action, sélectionnez une seconde action qu'OfficeScan doit effectuer si le nettoyage échoue. Si la première action n'est pas «Nettoyer», aucune seconde action n'est configurable.

Si la première action que vous choisissez est « Nettoyer », OfficeScan exécute la deuxième action lorsqu'il détecte des virus/programmes malveillants potentiels.

Utilisez une action spécifique pour chaque type de virus/ programme malveillant

Sélectionner manuellement une action de scan pour chaque type de virus/programme malveillant.

Pour tous les types de virus/programmes malveillants, à l'exception de ceux qui sont potentiels, toutes les actions de scan sont disponibles. Si vous choisissez «Nettoyer» comme première action, sélectionnez une seconde action qu'OfficeScan doit effectuer si

le nettoyage échoue. Si la première action n'est pas «Nettoyer», aucune seconde action n'est configurable.

Pour les virus et programmes malveillants potentiels, toutes les actions de scan sont disponibles, à l'exception de « Nettoyer ».

Répertoire de quarantaine

Si l'action concernant un fichier infecté est « Mettre en quarantaine », l'agent OfficeScan chiffre le fichier et le déplace vers un dossier de quarantaine temporaire situé dans le répertoire <*dossier d'installation de l'agent*>`\SUSPECT`, puis l'envoie vers le répertoire de quarantaine désigné.



Remarque

Vous pouvez restaurer des fichiers encodés en quarantaine si vous devez y accéder par la suite. Pour obtenir des informations détaillées, voir *Restauration des fichiers chiffrés à la page 7-47*.

Acceptez le répertoire de quarantaine par défaut, qui se trouve sur l'ordinateur du serveur OfficeScan. Le répertoire est au format URL. Il contient le nom d'hôte du serveur ainsi que l'adresse IP.

- Si le serveur gère simultanément des agents IPv4 et IPv6, utilisez le nom d'hôte de façon à ce que tous les agents puissent envoyer des fichiers mis en quarantaine vers le serveur.
- Si le serveur dispose uniquement d'une adresse IPv4 ou qu'il est identifié par celle-ci, seuls les agents IPv4 purs et à double pile peuvent envoyer des fichiers mis en quarantaine vers le serveur.
- Si le serveur dispose uniquement d'une adresse IPv6 ou qu'il est identifié par celle-ci, seuls les agents IPv6 purs et à double pile peuvent envoyer des fichiers mis en quarantaine vers le serveur.

Vous pouvez également définir un autre répertoire de quarantaine en saisissant l'emplacement au format URL, chemin UNC ou chemin de fichier absolu. Il convient que les agents aient la possibilité de se connecter à ce répertoire alternatif. Par exemple, le répertoire alternatif doit avoir une adresse IPv6 s'il est susceptible de recevoir des

fichiers mis en quarantaine d'agents IPv6 purs et à double pile. Trend Micro vous recommande de concevoir un répertoire double-pile alternatif, qui sera identifié par son nom d'hôte et pour lequel vous utiliserez le chemin UNC lorsque vous le saisirez.

Reportez-vous au tableau suivant pour obtenir de l'aide sur l'utilisation d'une URL, d'un chemin UNC ou d'un chemin de fichier absolu :

Tableau 7-14. Répertoire de quarantaine

Répertoire de quarantaine	Format accepté	Exemple	Remarques
Répertoire installé sur l'ordinateur connecté au serveur OfficeScan	URL	`http://<osceserver>`	Il s'agit du répertoire par défaut. Configurez les paramètres de ce répertoire, comme la taille du dossier de quarantaine. Pour obtenir des informations détaillées, voir *Gestionnaire de quarantaine à la page 13-57*.
	Chemin UNC	`\\<osceserver>\ofcscan\Virus`	
Un répertoire sur un autre ordinateur serveur OfficeScan (si vous avez d'autres serveurs OfficeScan sur votre réseau)	URL	`http://<osceserver2>`	Vérifiez que les agents peuvent se connecter à ce répertoire. Si vous spécifiez un répertoire non valide, l'agent OfficeScan conserve les fichiers en quarantaine dans le dossier SUSPECT jusqu'à ce que vous indiquiez un répertoire de quarantaine valide. Dans les journaux de virus/programmes malveillants du serveur, le résultat de scan est «Impossible d'envoyer le fichier en quarantaine vers le dossier de quarantaine spécifié». Si vous utilisez un chemin UNC, vérifiez que le répertoire de quarantaine est partagé avec le groupe «Tous» et que vous avez attribué des privilèges de lecture et d'écriture à ce groupe.
	Chemin UNC	`\\<osceserver2>\ofcscan\Virus`	
Autre endpoint du réseau	Chemin UNC	`\\<nom_ordinateur>\temp`	
Autre répertoire se trouvant sur l'agent OfficeScan	Chemin de fichier absolu	`C:\temp`	

Sauvegardez les fichiers avant nettoyage

Si OfficeScan est configuré pour nettoyer un fichier infecté, il peut commencer par le sauvegarder. Ceci vous permet de restaurer le fichier si vous devez y accéder par la suite. OfficeScan chiffre le fichier de sauvegarde pour empêcher son ouverture, puis le stocke dans le répertoire <*dossier d'installation de l'agent*>`\Backup`.

Pour restaurer des fichiers de sauvegarde encodés, reportez-vous à *Restauration des fichiers chiffrés à la page 7-47*.

Damage Cleanup Services

Damage Cleanup Services débarrasse les ordinateurs des virus basés sur fichiers et des virus de réseau, ainsi que des résidus de virus et de vers (chevaux de Troie, entrées de registre et fichiers viraux).

Selon le type de scan utilisé, l'agent déclenche Damage Cleanup Services avant ou après la détection de virus/programmes malveillants.

- Lorsque le scan est de type manuel, programmé ou immédiat, l'agent OfficeScan active d'abord Damage Cleanup Services, puis procède à la détection des virus/ programmes malveillants. Au cours de la détection de virus/programmes malveillants, l'agent est susceptible de déclencher à nouveau Damage Cleanup Services s'il doit procéder à un nettoyage.
- Pendant un scan en temps réel, l'agent OfficeScan procède tout d'abord à la détection de virus/programmes malveillants, puis déclenche Damage Cleanup Services s'il doit procéder à un nettoyage.

Vous pouvez sélectionner le type de nettoyage effectué par Damage Cleanup Services :

- **Nettoyage standard** : l'agent OfficeScan exécute l'une des actions suivantes au cours du nettoyage standard :
    - Détecte et supprime les chevaux de Troie actifs
    - Élimine les processus créés par les chevaux de Troie
    - Répare les fichiers système modifiés par les chevaux de Troie
    - Supprime les fichiers et les applications laissés par les chevaux de Troie

- **Nettoyage avancé** : outre les actions de nettoyage standard, l'agent OfficeScan interrompt les activités de logiciels de sécurité non autorisés, connus également sous le nom de « FakeAV », et certaines variantes de rootkits. L'agent OfficeScan utilise également des règles de nettoyage avancées afin de détecter et d'arrêter de manière proactive les applications qui présentent un comportement de FakeAV ou de rootkit.



Remarque

Tout en assurant une protection proactive, le nettoyage avancé génère également un nombre élevé de faux-positifs.

Damage Cleanup Services ne procède pas au nettoyage des virus et programmes malveillants potentiels, sauf si vous sélectionnez l'option **Exécuter la fonction Nettoyage dès qu'un virus/programme malveillant est détecté**. Vous pouvez sélectionner cette action uniquement si l'action appliquée aux virus/programmes malveillants potentiels n'est pas **Ignorer**, ni **Refuser l'accès**. Par exemple, si l'agent OfficeScan détecte un virus ou un programme malveillant potentiel au cours d'un scan en temps réel et que l'action définie est Mettre en quarantaine, l'agent OfficeScan met tout d'abord le fichier infecté en quarantaine, puis procède au nettoyage si nécessaire. Le type de nettoyage (standard ou avancé) dépend de l'option que vous avez choisie.

Afficher un message de notification lorsqu'un virus/ programme malveillant est détecté

Quand OfficeScan détecte un virus/programme malveillant au cours d'un scan en temps réel et d'un scan programmé, il peut afficher un message de notification pour informer l'utilisateur de la détection.

Pour modifier le message de notification, sélectionnez **Virus/Programmes malveillants** dans la liste déroulante **Type** sous **Administration** > **Notifications** > **Agent**.

Afficher un message de notification lorsqu'un virus/ programme malveillant potentiel est détecté

Quand OfficeScan détecte un virus/programme malveillant potentiel au cours d'un scan en temps réel et d'un scan programmé, il peut afficher un message de notification pour informer l'utilisateur de la détection.

Pour modifier le message de notification, sélectionnez **Virus/Programmes malveillants** dans la liste déroulante **Type** sous **Administration** > **Notifications** > **Agent**.

Restauration de fichiers mis en quarantaine

Vous pouvez restaurer des fichiers mis en quarantaine par OfficeScan si vous estimez que la détection a fait une erreur. La fonctionnalité de restauration de fichiers depuis la mise en quarantaine centrale vous permet de rechercher des fichiers mis dans le répertoire de quarantaine et d'effectuer une vérification SHA1 afin de vous assurer que les fichiers que vous souhaitez restaurer n'ont subi aucune modification.

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, sélectionnez un domaine ou un agent.
3. Cliquez sur **Tâches** > **Restauration depuis la mise en quarantaine centrale**.

   L'écran **Critères de restauration depuis la mise en quarantaine centrale** s'affiche.
4. Saisissez le nom de l'élément que vous souhaitez restaurer dans le champ **Fichier/ Objet infecté**.
5. Vous avez également la possibilité d'indiquer une période, le nom d'une menace de sécurité et le chemin d'accès de l'élément.
6. Cliquez sur **Rechercher**.

   L'écran **Restauration depuis la mise en quarantaine centrale** s'affiche et indique les résultats de la recherche.

7. Sélectionnez **Ajouter le fichier restauré à la liste des exclusions au niveau du domaine** afin de vous assurer que tous les agents OfficeScan du ou des domaines dans lesquels est restauré le fichier ajoutent ce fichier à la liste des exclusions de scan.

   Cela empêchera OfficeScan de détecter à nouveau ce fichier en tant que menace lors des futurs scans.

8. Vous avez également la possibilité de saisir la valeur SHA1 du fichier à des fins de vérification.

9. Sélectionnez le fichier à restaurer dans la liste et cliquez sur **Restaurer**.



Conseil

Pour afficher les agents OfficeScan sur lesquels le fichier est restauré, cliquez sur le lien qui se trouve dans la colonne **Endpoints**.

10. Cliquez sur **Fermer** dans la boîte de dialogue de confirmation.

    Pour vérifier qu'OfficeScan a bien restauré le fichier mis en quarantaine, voir *Affichage des journaux de restauration depuis la mise en quarantaine centrale à la page 7-100*.

Restauration des fichiers chiffrés

Pour empêcher son ouverture, OfficeScan encode un fichier infecté dans les cas suivants :

- Avant de placer un fichier en quarantaine
- Lors de la sauvegarde d'un fichier avant de le nettoyer

OfficeScan fournit un outil qui déchiffre, puis restaure le fichier si vous devez absolument extraire les informations qu'il contient. OfficeScan peut déchiffrer, puis restaurer les fichiers suivants :

TABLEAU 7-15. Fichiers qu'OfficeScan peut déchiffrer et restaurer

FICHIER	DESCRIPTION
Fichiers mis en quarantaine sur le endpoint de l'agent	Ces fichiers se trouvent dans le dossier <*dossier d'installation de l'agent*>`\SUSPECT\Backup` et sont purgés automatiquement au bout de 7 jours. Ces fichiers sont également téléchargés dans le répertoire de quarantaine désigné sur le serveur OfficeScan.
Fichiers placés en quarantaine dans le répertoire de quarantaine désigné	Par défaut, ce répertoire se trouve sur l'ordinateur du serveur OfficeScan. Pour obtenir des informations détaillées, voir *Répertoire de quarantaine à la page 7-42*.
Fichiers chiffrés sauvegardés	Il s'agit de la sauvegarde des fichiers infectés qu'OfficeScan a réussi à nettoyer. Ces fichiers se trouvent dans le dossier `<dossier d'installation de l'agent>\Backup`. Pour restaurer ces fichiers, les utilisateurs doivent les déplacer vers le dossier `<dossier d'installation de l'agent>\SUSPECT\Backup`. OfficeScan ne sauvegarde et ne chiffre les fichiers avant de les nettoyer que si vous sélectionnez **Sauvegarder les fichiers avant nettoyage** dans l'onglet **Agents** > **Gestion des agents > Paramètres** > **Paramètres de scan** > **{Type de scan}** > **Action**.



AVERTISSEMENT!

Lorsque vous restaurez un fichier infecté, le virus/programme malveillant qu'il contient peut se propager à d'autres fichiers ou ordinateurs. Avant de restaurer le fichier, isolez le endpoint infecté et déplacez les fichiers importants de ce endpoint vers un emplacement de sauvegarde.

Décryptage et restauration des fichiers

Procédure

- Si le fichier se trouve sur le endpoint de l'agent OfficeScan :

    a. Ouvrez une invite de commandes et accédez au <*dossier d'installation de l'agent*>.

b. Exécutez `VSEncode.exe` en double-cliquant sur le fichier ou en saisissant ce qui suit dans une invite de commandes :

```
VSEncode.exe /u
```

Ce paramètre ouvre un écran contenant la liste des fichiers qui se trouvent dans le répertoire `<dossier d'installation de l'agent>\SUSPECT\Backup`.

c. Sélectionnez un fichier à restaurer et cliquez sur **Restaurer**. L'outil ne peut restaurer qu'un seul fichier à la fois.

d. Dans l'écran qui s'affiche, indiquez le dossier dans lequel vous voulez restaurer le fichier.

e. Cliquez sur **OK**. Le fichier est restauré dans le dossier spécifié.



Remarque

Il se peut qu'OfficeScan scanne de nouveau le fichier et le considère comme infecté dès sa restauration. Pour éviter qu'il ne soit scanné, ajoutez-le à la liste d'exclusion de scan. Voir *Exclusions de scan à la page 7-33* pour obtenir des informations détaillées.

f. Cliquez sur **Fermer** lorsque vous avez terminé de restaurer des fichiers.

- Si le fichier se trouve sur le serveur OfficeScan ou dans un répertoire de quarantaine personnalisé :

a. Si le fichier se trouve sur l'ordinateur du serveur OfficeScan, ouvrez une invite de commandes et accédez au répertoire <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\VSEncrypt`.

Si le fichier se trouve dans un répertoire de quarantaine personnalisé, accédez au répertoire `<dossier d'installation du serveur>\PCCSRV\Admin\Utility` et copiez le dossier `VSEncrypt` sur le endpoint sur lequel se trouve le répertoire de quarantaine personnalisé.

b. Créez un fichier texte, puis saisissez le chemin d'accès complet des fichiers que vous souhaitez chiffrer ou déchiffrer.

À titre d'exemple, vous pouvez saisir le chemin d'accès `C:\Mes documents \Reports, \*.* dans le fichier texte pour restaurer tous les fichiers contenus dans C:\Mes documents\Reports`.

Les fichiers placés en quarantaine sur l'ordinateur du serveur OfficeScan se trouvent dans le répertoire `<dossier d'installation du serveur> \PCCSRV\Virus`.

c. Enregistrez le fichier texte avec une extension `INI` ou `TXT`. Par exemple, enregistrez-le sous `ForEncryption.ini` sur le lecteur `C:` C:.

d. Ouvrez une invite de commandes et accédez au répertoire dans lequel se trouve le dossier `VSEncrypt`.

e. Exécutez `VSEncode.exe` en saisissant :

```
VSEncode.exe /d /i <emplacement du fichier INI ou TXT>
```

Où :

`<emplacement du fichier INI ou TXT>` est le chemin d'accès du fichier `INI` ou `TXT` que vous avez créé (par exemple, `C:\ForEncryption.ini`).

f. Utilisez les autres paramètres pour lancer diverses commandes.

TABLEAU 7-16. Paramètres de restauration

PARAMÈTRE	DESCRIPTION
Aucun (aucun paramètre)	Chiffrer les fichiers
/d	Décoder les fichiers
/debug	Créez un journal de débogage et enregistrez-le sur le endpoint. Sur le endpoint de l'agent OfficeScan, le journal de débogage `VSEncrypt.log` est créé dans le `<dossier d'installation de l'agent>`.
/o	Remplacer un fichier encodé ou décodé s'il existe déjà
/f <nom du fichier>	Encoder ou décoder un seul fichier

Paramètre	Description
/nr	Ne pas restaurer le nom de fichier original
/v	Afficher des informations concernant l'outil
/u	Lancer l'interface utilisateur de l'outil
/r <Dossier de destination>	Dossier dans lequel un fichier sera restauré
/s <Nom du fichier original>	Nom du fichier chiffré original

Par exemple, saisissez la commande `VSEncode [/d] [/debug]` pour déchiffrer les fichiers du dossier `Suspect` et créer un journal de débogage. Lorsque vous chiffrez ou déchiffrez un fichier, OfficeScan crée le fichier chiffré ou déchiffré dans le même dossier que le fichier source. Avant de déchiffrer ou de chiffrer un fichier, assurez-vous qu'il n'est pas verrouillé.

Actions de scan anti-spywares/graywares

L'action de scan qu'OfficeScan effectue dépend du type de scan qui a détecté le spyware/grayware. Si des actions spécifiques peuvent être configurées pour chaque type de virus/programmes malveillants, une seule action peut l'être pour tous les types de spywares/graywares (pour plus d'informations sur les différents types de spywares/graywares, voir *Spywares et graywares à la page 7-5*). Par exemple, lorsqu'OfficeScan détecte un type de spyware/grayware lors d'un scan manuel (type de scan), il nettoie (action) les ressources système affectées.



Remarque

Les actions de scan à effectuer sur les spywares/graywares sont configurables uniquement via la console Web. La console de l'agent OfficeScan ne permet pas d'accéder à ces paramètres.

Voici la liste des actions qu'OfficeScan peut effectuer pour lutter contre les graywares/graywares :

TABLEAU 7-17. Actions de scan anti-spywares/graywares

ACTION	DESCRIPTION
Nettoyer	OfficeScan met fin aux processus ou supprime les registres, fichiers, cookies et raccourcis. Après avoir nettoyé des spywares/graywares, les agents OfficeScan sauvegardent les données les concernant. Vous pouvez restaurer celles-ci si vous estimez que l'accès à ces spywares/graywares est sans danger. Voir *Restauration des spywares/graywares à la page 7-55* pour obtenir des informations détaillées.
Ignorer	OfficeScan n'effectue aucune action sur les composants de spyware/ grayware détectés mais consigne la détection de spyware/grayware dans les journaux. Cette action n'est possible que lors du scan manuel, du scan programmé et du scan immédiat. Lors du scan en temps réel, l'action est «Refuser l'accès». OfficeScan n'effectue aucune action si le spyware/grayware détecté fait partie de la liste approuvée. Voir *Liste des spywares/graywares approuvés à la page 7-52* pour obtenir des informations détaillées.
Refuser l'accès	OfficeScan refuse l'accès (copie, ouverture) aux composants de spyware/ grayware détectés. Cette action ne peut être effectuée que lors d'un scan en temps réel. Lors d'un scan manuel, d'un scan programmé et d'un scan immédiat, l'action est «Ignorer».

Afficher un message de notification lorsqu'un spyware/ grayware est détecté

Lorsque OfficeScan détecte un spyware/grayware au cours d'un scan en temps réel et d'un scan programmé, il peut afficher un message de notification pour informer l'utilisateur de la détection.

Pour modifier le message de notification, sélectionnez **Spywares/graywares** dans la liste déroulante **Type** sous **Administration** > **Notifications** > **Agent**.

Liste des spywares/graywares approuvés

OfficeScan fournit une liste des spywares/graywares «approuvés», qui contient les fichiers ou les applications que vous ne souhaitez pas voir considérés comme des

spywares ou des graywares. Lorsqu'un spyware/grayware particulier est détecté lors d'un scan, OfficeScan vérifie la liste des spywares/graywares approuvés et n'effectue aucune action si une correspondance est trouvée dans cette liste.

Appliquez la liste des spywares/graywares approuvés à un ou plusieurs agents et domaines, ou à tous les agents gérés par le serveur. La liste des spywares/graywares approuvés s'applique à tous les types de scan, ce qui signifie que la même liste approuvée sera utilisée lors du scan manuel, du scan en temps réel, du scan programmé et du scan immédiat.

Ajout de spywares/graywares détectés à la liste approuvée.

Procédure

1. Accédez à l'un des emplacements suivants :
   - **Agents** > **Gestion des agents**
   - **Journaux** > **Agents** > **Risques de sécurité**
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Journaux** > **Journaux de spywares/graywares** ou **Afficher journaux** > **Journaux de spywares/graywares**.
4. Spécifiez les critères de journaux, puis cliquez sur **Afficher les journaux**.
5. Sélectionnez les journaux et cliquez sur **Ajouter à la liste approuvée**.
6. Appliquez les spywares/graywares approuvés uniquement aux ordinateurs des agents sélectionnés ou à certains domaines.
7. Cliquez sur **Enregistrer**. Les agents sélectionnés appliquent les paramètres et le serveur OfficeScan ajoute les spywares/graywares à la liste des éléments approuvés qui se trouve sous **Agents** > **Gestion des agents > Paramètres** > **Liste des spywares/graywares approuvés**.



Remarque

OfficeScan peut ajouter un maximum de 1024 spywares/graywares à la liste des spywares/graywares approuvés.

Gestion de la liste des spywares/graywares approuvés

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Liste des spywares/graywares approuvés**.
4. Dans le tableau **Noms des spywares/graywares**, sélectionnez un nom de spyware/grayware. Pour sélectionner plusieurs noms, maintenez enfoncée la touche CTRL lors de la sélection.
    - Vous pouvez également entrer un mot clé dans le champ **Rechercher** et cliquer sur **Rechercher**. OfficeScan actualise le tableau avec les noms correspondant au mot clé.
5. Cliquez sur **Ajouter**.

    Les noms se déplacent dans le tableau **Liste approuvée**.
6. Pour supprimer les noms dans la liste des spywares/graywares approuvés, sélectionnez les noms et cliquez sur **Supprimer**. Pour sélectionner plusieurs noms, maintenez enfoncée la touche CTRL lors de la sélection.
7. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :
    - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.

- **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Restauration des spywares/graywares

Après avoir nettoyé les spywares/graywares, les agents OfficeScan sauvegardent les données des spywares/graywares. Demandez aux agents en ligne de restaurer les données sauvegardées si vous considérez que les données sont inoffensives. Sélectionnez les données de spyware/grayware à restaurer en fonction de l'heure de sauvegarde.



Remarque

Les utilisateurs d'agents OfficeScan ne peuvent pas lancer de restauration de spywares/graywares et ne sont pas informés des données de sauvegarde que l'agent a pu restaurer.

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, ouvrez un domaine, puis sélectionnez un agent.

   Remarque

   Un seul agent à la fois peut procéder à une restauration de spywares/graywares.

3. Cliquez sur **Tâches** > **Restauration de spywares/graywares**.
4. Pour afficher les éléments à restaurer pour chaque segment de données, cliquez sur **Afficher**.

   Un nouvel écran s'affiche. Cliquez sur **Précédent** pour revenir à l'écran précédent.

5. Sélectionnez les segments de données que vous souhaitez restaurer.
6. Cliquez sur **Restaurer**.

OfficeScan vous indique l'état de la restauration. Consultez les journaux de restauration des spywares/graywares pour obtenir un rapport complet. Voir *Affichage des journaux de restauration de spywares/graywares à la page 7-105* pour obtenir des informations détaillées.

Privilèges et autres paramètres de scan

Les utilisateurs ayant des privilèges de scan ont davantage de contrôle sur la manière dont les fichiers de leur ordinateur sont scannés. Les privilèges de scan permettent aux utilisateurs ou agents OfficeScan d'effectuer les tâches suivantes :

- Les utilisateurs peuvent configurer les paramètres de scan manuel, de scan programmé et de scan en temps réel. Pour obtenir des informations détaillées, voir *Privilèges de type de scan à la page 7-56*.
- Les utilisateurs peuvent différer, arrêter ou annuler un scan programmé. Pour obtenir des informations détaillées, voir *Privilèges et autres paramètres de scan programmé à la page 7-59*.
- Les utilisateurs peuvent activer le scan des messages électroniques POP3 pour détecter des virus/programmes malveillants. Pour obtenir des informations détaillées, voir *Privilèges et autres paramètres du scan de courrier à la page 7-65*.
- L'agent OfficeScan peut utiliser les paramètres du cache pour améliorer ses performances de scan. Pour obtenir des informations détaillées, voir *Paramètres du cache pour les scans à la page 7-67*.

Privilèges de type de scan

Permet aux utilisateurs de configurer leurs propres paramètres de scan manuel, de scan en temps réel et de scan programmé

Autorisation de privilèges de type de scan

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Dans l'onglet **Privilèges**, accédez à la section **Privilèges de scan**.
5. Sélectionnez les types de scan que les utilisateurs sont autorisés à configurer.
6. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :
    - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.
    - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Configuration des paramètres de scan pour les agents OfficeScan

Procédure

1. Cliquez avec le bouton droit de la souris sur l'icône de l'agent OfficeScan dans la barre d'état système et sélectionnez **Ouvrir la console de l'agent OfficeScan**.
2. Cliquez sur **Paramètres** > **{Type de scan}**.

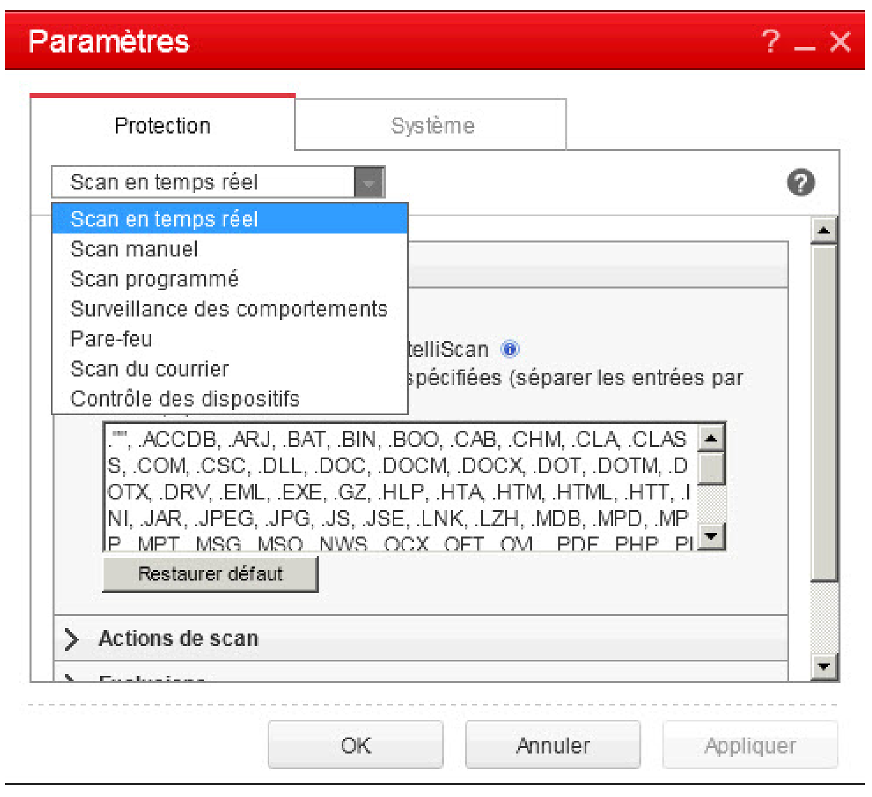


FIGURE 7-1. Paramètres de scan sur la console de l'agent OfficeScan

3. Configurez les paramètres suivants :

   - Paramètres de scan en temps réel : Action des utilisateurs sur les fichiers, Fichiers à scanner, Paramètres de scan, Exclusions de scan, Actions de scan

   - Paramètres de scan manuel : Fichiers à scanner, Paramètres de scan, Utilisation de l'unité centrale, Exclusions de scan, Actions de scan

   - Paramètres de scan programmé : Programme, Fichiers à scanner, Paramètres de scan, Utilisation de l'unité centrale, Exclusions de scan, Actions de scan

4. Cliquez sur **OK**.

Privilèges et autres paramètres de scan programmé

Si le scan programmé est configuré pour s'exécuter sur l'agent, les utilisateurs peuvent différer et ignorer/interrompre le scan programmé.

Différer le scan programmé

Les utilisateurs disposant du privilège « Différer le scan programmé » peuvent effectuer les actions suivantes:

- Différer le scan programmé avant qu'il ne débute et définir la durée du report. Le scan programmé ne peut être différé qu'une seule fois.
- Lorsque le scan programmé est en cours, les utilisateurs peuvent l'arrêter et le redémarrer ultérieurement. Les utilisateurs définissent alors la durée devant s'écouler avant le redémarrage du scan. Lorsque le scan reprend, tous les fichiers scannés précédemment sont à nouveau scannés. Le scan programmé peut être arrêté puis redémarré une seule fois.



Remarque

La durée de report minimale/le temps écoulé minimal que les utilisateurs peuvent définir est de 15 minutes. Le maximum est de 12 heures et 45 minutes, durée que vous pouvez réduire en accédant à **Agents** > **Paramètres généraux de l'agent**. Dans la section **Paramètres de scan programmé**, modifiez le paramètre **Différer le scan programmé de__ heures et __ minutes**.

Annuler et arrêter le scan programmé

Ce privilège permet aux utilisateurs d'effectuer les actions suivantes :

- Annuler un scan programmé avant qu'il ne débute
- Arrêter un scan programmé déjà en cours



Remarque

Les utilisateurs ne peuvent pas ignorer ni arrêter un scan programmé à plusieurs reprises. Même après un redémarrage du système, le scan programmé reprend, selon les paramètres de la prochaine exécution programmée.

Notification de privilège de scan programmé

Pour permettre aux utilisateurs de tirer profit des privilèges de scan programmé, rappelez-leur les privilèges que vous leur avez accordés en configurant OfficeScan pour qu'il affiche un message de notification avant l'exécution du scan programmé.

Attribution de privilèges de scan programmé et affichage de la notification de privilège

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Dans l'onglet **Privilèges**, allez à la section **Privilèges de scan programmé**.
5. Sélectionnez les options suivantes :
    - Différer le scan programmé
    - Annuler et arrêter le scan programmé
6. Cliquez sur l'onglet **Autres paramètres** et accédez à la section **Paramètres de scan programmé**.
7. Sélectionnez **Afficher un message de notification avant le début d'un scan programmé**.

    Lorsque vous activez cette option, un message de notification s'affiche sur le endpoint de l'agent quelques minutes avant que l'exécution du scan programmé.

Les utilisateurs sont informés de la programmation de scan (date et heure) et de leurs privilèges de scan programmé, notamment le report, l'annulation ou l'arrêt du scan programmé.



Remarque

Le nombre de minutes peut être configuré. Pour configurer le nombre de minutes, accédez à **Agents** > **Paramètres généraux de l'agent**. Dans la section **Paramètres de scan programmé**, modifiez le paramètre **Rappeler le scan programmé aux utilisateurs __ minutes avant qu'il n'exécute le paramètre** .

8. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :

    - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.

    - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Report/Annulation et arrêt du scan programmé sur l'agent

Procédure

- Si le scan programmé n'a pas encore démarré :

    a. Cliquez avec le bouton droit de la souris sur l'icône de l'agent OfficeScan dans la barre d'état système et sélectionnez **Configuration avancée du scan programmé**.

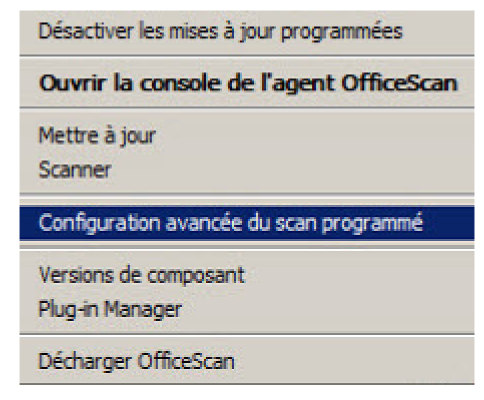


FIGURE 7-2. Option Paramètres avancés de scan programmé



Remarque

Les utilisateurs n'ont pas besoin d'effectuer cette étape si le message de notification est activé et configuré pour s'afficher quelques minutes avant que le scan programmé ne s'exécute. Pour plus de détails sur le message de notification, reportez-vous à *Notification de privilège de scan programmé à la page 7-60*.

b. Dans la fenêtre de notification qui s'affiche, sélectionnez l'une des options suivantes :

- **Différer le scan de __ heures et __ minutes.**
- **Annuler ce scan programmé. Le prochain scan programmé s'exécutera le <date> à <heure>.**

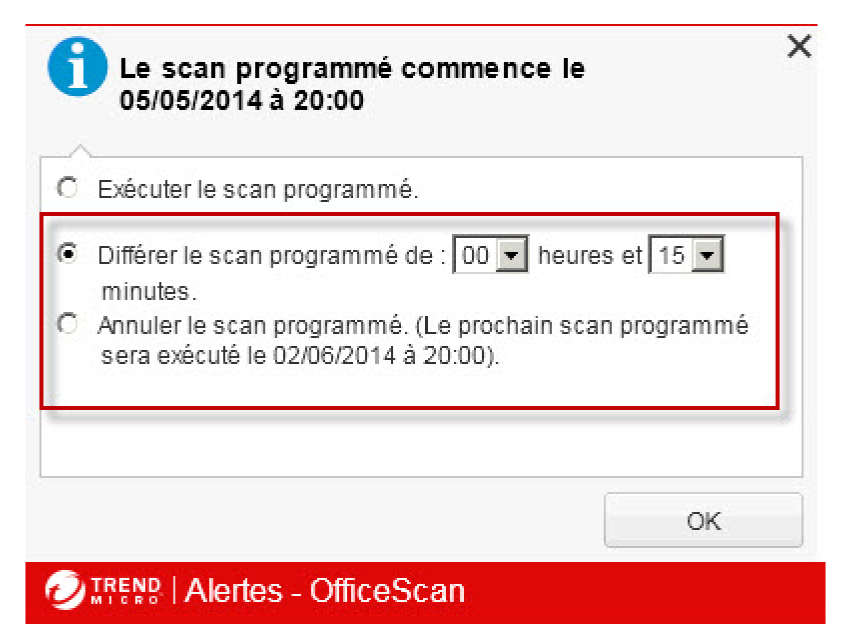


FIGURE 7-3. Privilèges de scan programmé sur le endpoint de l'agent OfficeScan

- Si le scan programmé est en cours :

  a. Cliquez avec le bouton droit de la souris sur l'icône de l'agent OfficeScan dans la barre d'état système et sélectionnez **Paramètres avancés de scan programmé**.

  b. Dans la fenêtre de notification qui s'affiche, sélectionnez l'une des options suivantes :

  - **Arrêter le scan. Redémarrer le scan après __ heures et __ minutes.**
  - **Arrêter le scan. Le prochain scan programmé s'exécutera le <date> à <heure>.**

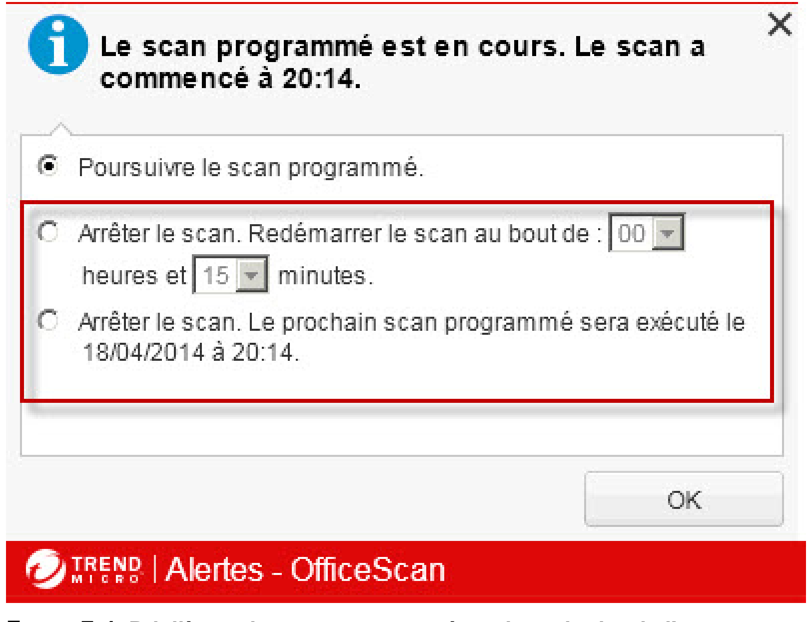


Figure 7-4. Privilèges de scan programmé sur le endpoint de l'agent OfficeScan

Privilèges et autres paramètres du scan de courrier

Si les agents disposent des privilèges de scan du courrier, l'onglet **Scan du courrier** s'affiche sur la console de l'agent OfficeScan. L'option **Scan du courrier** affiche le scan du courrier POP3.

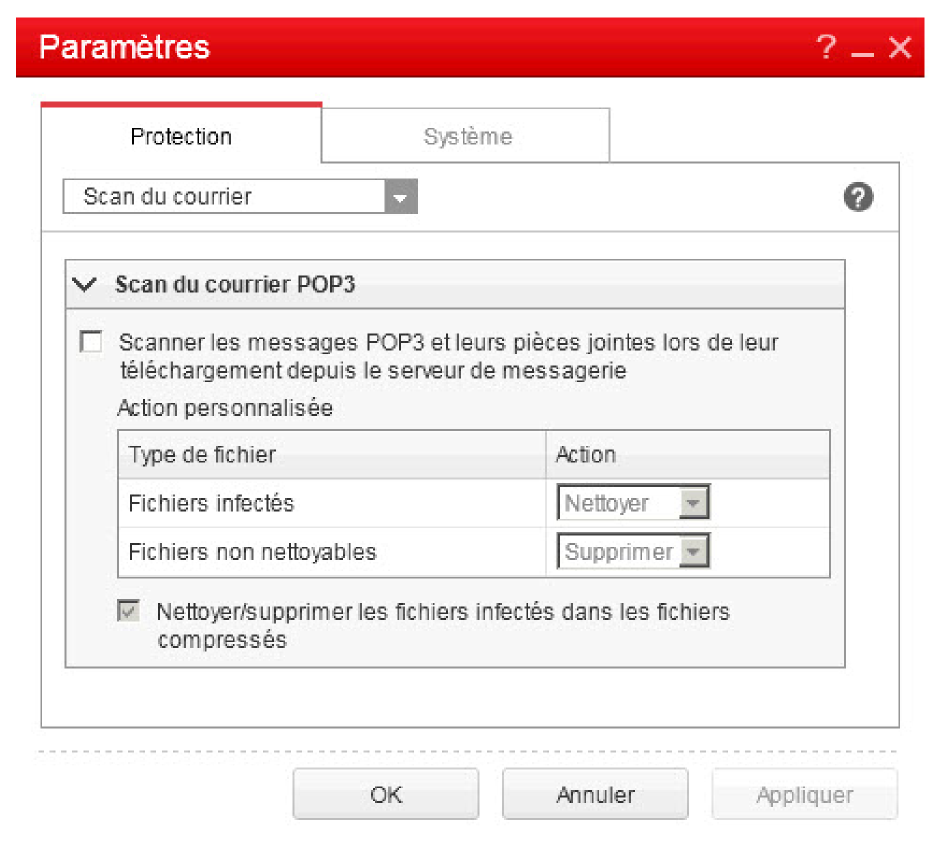


FIGURE 7-5. Paramètres de scan du courrier sur la console de l'agent OfficeScan

Le tableau suivant décrit le programme de scan du courrier POP3.

TABLEAU 7-18. Programmes de scan de messagerie

DÉTAILS	DESCRIPTION
Objet	Scanne les messages de la boîte POP3 à la recherche de virus/programmes malveillants.
Prérequis	• Doit être activé par les administrateurs à partir de la console Web au préalable. **Remarque** Pour activer le scan de la messagerie POP3, voir *Attribution des privilèges du scan de courrier et activation du scan de la messagerie POP3 à la page 7-66*. • Action à entreprendre contre les virus/programmes malveillants, à définir à l'aide de la console de l'agent OfficeScan, mais pas de la console Web
Types de scan pris en charge	Scan en temps réel Le scan s'effectue lors de la récupération des messages électroniques à partir du serveur de messagerie POP3.
Résultats de scan	• Informations relatives aux risques de sécurité détectés, disponibles après l'exécution du scan. • Résultats de scan non consignés dans l'écran **Journaux** de la console de l'agent OfficeScan • Résultats de scan non envoyés au serveur.
Autres informations	Partage le service proxy d'OfficeScan NT (`TMProxy.exe`) avec la fonction d'évaluation de réputation des sites Web.

Attribution des privilèges du scan de courrier et activation du scan de la messagerie POP3

Procédure

1. Accédez à **Agents** > **Gestion des agents**.

2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.

3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.

4. Dans l'onglet **Privilèges**, accédez à la section **Scan du courrier**.

5. Sélectionnez **Afficher les paramètres Scan du courrier sur la console de l'agent**.

6. Cliquez sur l'onglet **Autres paramètres** et accédez à la section **Paramètres de scan de la messagerie POP3**.

7. Sélectionnez **Scanner la messagerie POP3**.

8. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :

    - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.

    - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Paramètres du cache pour les scans

L'agent OfficeScan peut générer des fichiers de cache de scan à la demande et des fichiers de signature numérique pour améliorer les performances du scan. Lors de l'exécution d'un scan à la demande, l'agent OfficeScan vérifie tout d'abord le fichier de cache de signature numérique, puis le fichier de cache de scan à la demande, pour déterminer les fichiers à exclure du scan. La durée du scan est réduite si de nombreux fichiers sont exclus du scan.

Cache de signature numérique

Le fichier de cache de signature numérique est utilisé lors du scan manuel, du scan programmé et du scan immédiat. Les agents ne scannent pas les fichiers dont les signatures ont été ajoutées au fichier de cache de signature numérique.

L'agent OfficeScan applique le même modèle de signature numérique que celui utilisé pour la surveillance des comportements afin de générer le fichier de cache de signature numérique. Le Digital Signature Pattern contient une liste de fichiers que Trend Micro estime fiables et qui sont, par conséquent, exclus des scans.



Remarque

La surveillance des comportements est désactivée pour les plateformes de serveur Windows (prise en charge des plate-formes 64 bits pour Windows XP, 2003, et Vista sans SP1 non disponible). Si le cache de signature numérique est activé, les agents OfficeScan de ces plates-formes téléchargent le modèle de signature numérique en vue d'une utilisation dans le cache, mais ne téléchargent pas les autres composants de surveillance des comportements.

Les agents génèrent le fichier de cache de signature numérique selon la programmation, configurable à partir de la console Web. Cela permet aux agents de :

- Ajouter les signatures des nouveaux fichiers intégrés au système depuis la génération du dernier fichier de cache
- Supprimer les signatures des fichiers qui ont été modifiés ou supprimés du système

Pendant le processus de génération du cache, les agents recherchent dans les dossiers suivants les fichiers fiables, puis ajoutent les signatures de ces fichiers au fichier de cache de signature numérique :

- `%PROGRAMFILES%`
- `%WINDIR%`

Le processus de génération de cache n'affecte pas les performances du endpoint car les agents consomment des ressources système restreintes au cours de ce processus. Les agents sont également en mesure de reprendre une tâche de génération de cache ayant

été interrompue pour un motif quelconque (par exemple, en cas d'arrêt de l'ordinateur hôte ou de débranchement de l'adaptateur secteur d'un endpoint sans fil).

Mémoire cache du scan à la demande

Le fichier de cache de scan à la demande est utilisé lors du scan manuel, du scan programmé et du scan immédiat. Les agents OfficeScan ne scannent pas les fichiers dont les caches ont été ajoutés au fichier de cache de scan à la demande.

À chaque exécution du scan, l'agent OfficeScan vérifie les propriétés des fichiers ne présentant pas de menaces. Si un fichier fiable n'a pas été modifié depuis un certain temps (période à configurer), l'agent OfficeScan ajoute le cache de ce fichier au fichier de cache de scan à la demande. Lors du scan suivant, le fichier n'est pas scanné si son cache n'a pas expiré.

Le cache d'un fichier fiable expire au bout d'un certain nombre de jours (période également à configurer). Lorsque le scan est exécuté pendant ou après l'expiration du cache, l'agent OfficeScan supprime le cache expiré et scanne le fichier à la recherche de menaces. Si le fichier ne présente aucune menace et qu'aucune modification n'y a été apportée, le cache de ce fichier est de nouveau ajouté au fichier de cache de scan à la demande. Si le fichier ne présente aucune menace, mais qu'une modification y a été récemment apportée, le cache n'est pas ajouté et ce fichier sera scanné lors du prochain scan.

Un cache de fichier fiable expire pour éviter que des fichiers infectés ne soient exclus des scans, comme l'illustrent les exemples suivants :

- Il est possible qu'un fichier de signatures trop ancien ait considéré un fichier infecté non modifié comme ne présentant aucune menace. S'il n'y a pas d'expiration de cache, le fichier infecté reste dans le système jusqu'à ce qu'il soit modifié et détecté par un scan en temps réel.
- Si un fichier mis en cache a été modifié et que le scan en temps réel ne fonctionne pas depuis la modification du fichier, il est nécessaire que le cache expire pour que le fichier modifié puisse être scanné à la recherche de menaces.

Le nombre de caches ajoutés au fichier de cache de scan à la demande dépend du type de scan et de la cible visée. Par exemple, le nombre de caches peut être réduit si l'agent OfficeScan scanne uniquement 200 fichiers sur 1 000 d'un endpoint au cours d'un scan manuel.

Si l'exécution de scans à la demande est fréquente, le fichier de cache de scan à la demande réduit la durée de scan de façon significative. Au cours d'une tâche de scan pour laquelle aucun cache n'a expiré, la durée d'un scan demandant généralement 12 minutes peut être réduite à 1 minute. Pour améliorer les performances, vous pouvez réduire le nombre de jours pendant lequel un fichier n'a pas à être modifié et prolonger la période d'expiration du cache. Étant donné que les fichiers doivent rester inchangés pendant une période relativement courte, vous pouvez ajouter un nombre de caches plus important au fichier de cache. La période d'expiration des caches est également plus longue, ce qui signifie qu'un nombre de fichiers plus important est ignoré au cours de scans.

Si les scans à la demande ne sont que rarement exécutés, vous pouvez désactiver la mémoire cache du scan à la demande car les caches expireront avant l'exécution du prochain scan.

Configuration des paramètres du cache pour les scans

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine (icône) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Cliquez sur l'onglet **Autres paramètres** et accédez à la section **Paramètres du cache pour les scans**.
5. Configurez les paramètres applicables au cache de signature numérique.
    a. Sélectionnez **Activer le cache de la signature numérique**.
    b. Dans la zone **Générer le cache tous les __ jours**, indiquez la fréquence à laquelle l'agent génère le cache.
6. Configurez les paramètres applicables au cache de scan à la demande.
    a. Sélectionnez **Activer le cache du Scan à la demande**.

b. Dans la zone **Ajouter le cache pour les fichiers légitimes qui n'ont pas été modifiés depuis __ jours**, spécifiez le nombre de jours pendant lequel un fichier doit rester inchangé avant qu'il ne soit mis en cache.

c. Dans la zone **Le cache de tous les fichiers légitimes expire dans __ jours**, indiquez la période maximale en jours pendant laquelle un cache reste dans le fichier de cache.



Remarque

Pour éviter que les caches ajoutés au cours d'un scan n'expirent le même jour, les caches expirent de façon aléatoire au cours de la période maximale en jours que vous avez spécifiée. Par exemple, si 500 fichiers sont ajoutés au cache aujourd'hui et que la période maximale spécifiée est de 10 jours, une partie des caches expirera demain, et la majorité d'entre eux, au cours des jours suivants. Au dixième jour, tous les caches restants expireront.

7. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :

- **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.
- **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Paramètres de scan généraux

Des paramètres de scan généraux peuvent être appliqués aux agents de diverses manières.

- Un paramètre de scan donné peut s'appliquer à tous les agents gérés par le serveur ou uniquement aux agents disposant de certains privilèges de scan. Par exemple, si

vous configurez la durée du report du scan programmé, seuls les agents disposant du privilège les autorisant à reporter le scan programmé seront concernés par ce paramètre.

- Un paramètre de scan donné peut s'appliquer à tous les types de scan ou à un type particulier. Par exemple, dans le cas de endpoints sur lesquels le serveur OfficeScan et l'agent OfficeScan sont tous deux installés, vous pouvez exclure du scan la base de données du serveur OfficeScan. Cependant, ce paramètre ne s'applique que durant les scans en temps réel.
- Un paramètre de scan donné peut s'appliquer aux recherches de virus/programmes malveillants, aux recherches de spywares/graywares, ou aux deux types de recherche. Le mode d'évaluation, par exemple, ne s'applique qu'aux scans visant à détecter des spywares/graywares.

Configuration des paramètres de scan généraux

Procédure

1. Accédez à **Agents** > **Paramètres généraux de l'agent**.
2. Configurez les paramètres de scan généraux dans chacune des sections disponibles.
   - *Section des paramètres de scan à la page 7-72*
   - *Section des paramètres de scan programmé à la page 7-79*
   - *Section des paramètres de bande passante des journaux de virus/programmes malveillants à la page 7-82*
3. Cliquez sur **Enregistrer**.

Section des paramètres de scan

La section **Paramètres de scan** des de l'écran **Paramètres généraux de l'agent** permet aux administrateurs de configurer ce qui suit :

- *Ajouter le scan manuel au menu des raccourcis Windows sur les agents OfficeScan à la page 7-73*

Ajouter le scan manuel au menu des raccourcis Windows sur les agents OfficeScan

Lorsque ce paramètre est activé, tous les agents OfficeScan gérés par le serveur ajoutent une option **Scanner avec OfficeScan** au menu de l'Explorateur Windows accessible avec le bouton droit de la souris. Lorsque les utilisateurs cliquent avec le bouton droit sur un fichier ou un dossier sur le bureau de Windows ou dans l'Explorateur Windows et sélectionnent l'option, le scan manuel scanne le fichier ou le dossier pour rechercher les virus/programmes malveillants et les spywares/graywares.

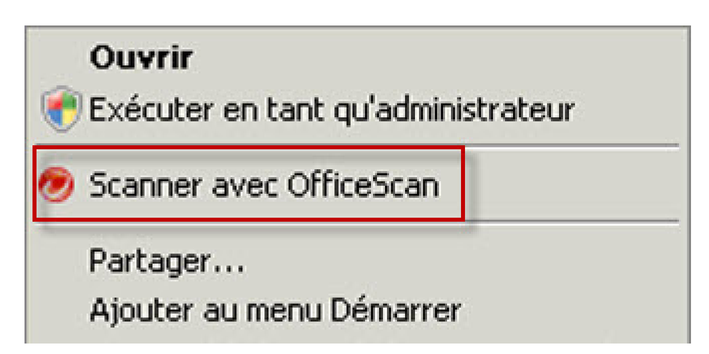


FIGURE 7-6. Option Scanner avec OfficeScan

Exclure du scan en temps réel la base de données du serveur OfficeScan

Si l'agent OfficeScan et le serveur OfficeScan sont installés sur le même endpoint, l'agent OfficeScan ne scannera pas la base de données du serveur pour y rechercher des virus/programmes malveillants et des spywares/graywares lors du scan en temps réel.



Conseil

Activez ce paramètre pour empêcher toute détérioration de la base de données susceptible de se produire lors du scan.

Exclure des scans les dossiers et les fichiers du serveur Microsoft Exchange

Si l'agent OfficeScan et un serveur Microsoft Exchange 2000/2003 sont installés sur le même endpoint, OfficeScan ne scannera pas les dossiers et les fichiers suivants de Microsoft Exchange pour y rechercher des virus/programmes malveillants et des spywares/graywares lors du scan manuel, en temps réel, programmé et immédiat :

- Les dossiers suivants qui se trouvent sous `\Exchsrvr\Mailroot\vsi 1` : `Queue`, `PickUp` et `BadMail`
- `.\Exchsrvr\mdbdata`, y compris ces fichiers : `priv1.stm`, `priv1.edb`, `pub1.stm` et `pub1.edb`
- `.\Exchsrvr\Storage Group`

Pour les dossiers de Microsoft Exchange 2007 ou version supérieure, vous devez ajouter manuellement les dossiers à la liste d'exclusion de scan. Pour plus d'informations sur les exclusions de scan, consultez le site Web suivant :

http://technet.microsoft.com/en-us/library/bb332342.aspx

Voir *Exclusions de scan à la page 7-33* pour connaître les étapes de configuration de la liste d'exclusion de scan.

Activer le scan différé pour les opérations de fichier

Les administrateurs peuvent configurer OfficeScan pour différer le scan de fichiers. OfficeScan permet à l'utilisateur de copier des fichiers, puis scanne les fichiers lorsque la copie est terminée. Ce scan différé améliore les performances des processus de copie et de scan.



Remarque

Le scan différé nécessite la version 9.713 (ou une version ultérieure) du moteur de scan antivirus (VSAPI). Pour plus de détails sur la mise à niveau du serveur, reportez-vous à *Mise à jour manuelle du serveur OfficeScan à la page 6-29*.

Configurer les paramètres de scan pour les gros fichiers compressés

Tous les agents OfficeScan gérés par le serveur vérifient les paramètres suivants lorsqu'ils scannent des fichiers compressés à la recherche de virus/programmes malveillants et de spywares/graywares lors du scan manuel, du scan en temps réel, du scan programmé et du scan immédiat :

- **Configurer les paramètres de scan pour les fichiers compressés volumineux** : sélectionnez cette option pour activer le traitement des fichiers compressés.
- Configurez les paramètres suivants séparément pour le scan en temps réel et les autres types de scans (manuel, programmé et immédiat) :
  - **Ne pas scanner les fichiers (inclus dans un fichier compressé) si la taille dépasse __ Mo** : OfficeScan ne scanne pas les fichiers dont la taille dépasse la limite indiquée.
  - **Dans un fichier compressé, scanner uniquement les __ premiers fichiers** : après la décompression d'un fichier compressé, OfficeScan scanne le nombre de fichiers spécifié et ignore les fichiers restants.

Nettoyer/supprimer les fichiers infectés dans les fichiers compressés

Lorsque tous les agents gérés par le serveur détectent des virus/programmes malveillants dans des fichiers compressés lors du scan manuel, en temps réel,

programmé ou immédiat et que les conditions suivantes sont remplies, les agents nettoient ou suppriment les fichiers infectés.

- « Nettoyer » ou « Supprimer » est l'action qu'OfficeScan doit effectuer. Vérifiez l'action entreprise par OfficeScan à l'encontre des fichiers infectés en accédant à l'onglet **Agents** > **Gestion des agents > Paramètres** > **Paramètres de scan** > **{Type de scan}** > **Action**.
- Activez ce paramètre. L'activation de ce paramètre est susceptible d'augmenter l'utilisation des ressources du endpoint pendant le scan qui peut, de ce fait, durer plus longtemps. Ceci est dû au fait qu'OfficeScan doit décompresser le fichier compressé, nettoyer/supprimer les fichiers infectés qu'il contient, puis le compresser à nouveau.
- Le format de fichier compressé est pris en charge. OfficeScan ne prend en charge que certains formats de fichiers compressés, parmi lesquels figurent ZIP et Office Open XML, qui utilise les technologies de compression ZIP. Office Open XML est le format par défaut pour les applications Microsoft Office 2007 telles qu'Excel, PowerPoint et Word.



Remarque

Contactez votre service d'assistance pour obtenir une liste complète des formats de fichiers compressés pris en charge.

Par exemple, le scan en temps réel est configuré pour supprimer les fichiers infectés par un virus. Lorsque le scan en temps réel décompresse un fichier compressé nommé `abc.zip` et détecte dans celui-ci un fichier infecté nommé `123.doc` , OfficeScan supprime `123.doc`, puis compresse à nouveau `abc.zip`, qui est désormais accessible en toute sécurité.

Le tableau suivant décrit ce qui se passe lorsque l'une des conditions n'est pas remplie.

TABLEAU 7-19. Scénarios et résultats pour les fichiers compressés

ÉTAT DE « NETTOYER/ SUPPRIMER LES FICHIERS INFECTÉS DANS LES FICHIERS COMPRESSÉS »	ACTION QUE DOIT EFFECTUER OFFICESCAN	FORMAT DE FICHIER COMPRESSÉ	RÉSULTAT
Activé	Nettoyer ou Supprimer	Non pris en charge Exemple : `def.rar` contient un fichier infecté `123.doc`.	OfficeScan chiffre `def.rar`, mais ne nettoie pas, ne supprime pas et n'entreprend aucune autre action à l'encontre de `123.doc`.
Désactivé	Nettoyer ou Supprimer	Pris en charge/Non pris en charge Exemple : `abc.rar` contient un fichier infecté `123.doc`.	OfficeScan ne nettoie pas, ne supprime pas et n'entreprend aucune autre action à l'encontre de `abc.zip` et `123.doc`.

État de « Nettoyer/supprimer les fichiers infectés dans les fichiers compressés »	Action que doit effectuer OfficeScan	Format de fichier compressé	Résultat
Activé/ Désactivé	Ni Nettoyer ni Supprimer (en d'autres termes, l'une des actions suivantes : Renommer, Mettre en quarantaine, Refuser l'accès ou Ignorer)	Pris en charge/Non pris en charge Exemple : `abc.rar` contient un fichier infecté `123.doc`.	OfficeScan entreprend l'action configurée (Renommer, Mettre en quarantaine, Refuser l'accès ou Ignorer) à l'encontre du fichier `abc.zip` et pas du fichier `123.doc` Si l'action est : **Renommer** : OfficeScan modifie le nom du fichier `abc.zip` et le renomme `abc.vir`, mais ne renomme pas le fichier `123.doc`. **Quarantaine** : OfficeScan met en quarantaine `abc.zip` (`123.doc` et tous les fichiers non infectés sont mis en quarantaine). **Ignorer** : OfficeScan n'entreprend aucune action à l'encontre de `abc.zip` et `123.doc` mais consigne la détection de virus. **Refuser l'accès** : OfficeScan refuse l'accès à `abc.zip` lorsque l'on tente de l'ouvrir (`123.doc` et tous les fichiers non infectés ne peuvent pas être ouverts).

Activer le mode d'évaluation

En mode d'évaluation, tous les agents gérés par le serveur consignent les spywares/graywares détectés pendant le scan manuel, programmé, en temps réel et immédiat, mais

ne nettoient pas les composants de ces spywares/graywares. Le nettoyage met fin aux processus ou supprime les répertoires, fichiers, cookies et raccourcis.

Le mode d'évaluation de Trend Micro a été conçu pour vous permettre d'évaluer les éléments que Trend Micro détecte comme étant des spywares/graywares avant d'entreprendre une action en fonction de votre évaluation. Par exemple, les spywares/graywares détectés qui ne constituent pas selon vous un risque de sécurité peuvent être ajoutés à la liste des spywares/graywares approuvés.

En mode d'évaluation, OfficeScan effectue les actions de scan suivantes :

- **Ignorer** : pendant le scan manuel, le scan programmé et le scan immédiat
- **Refuser l'accès** : pendant le scan en temps réel



Remarque

Le mode d'évaluation a la priorité sur toute action de scan configurée par l'utilisateur. Par exemple, même si vous choisissez « Nettoyer » comme action lors du scan manuel, « Ignorer » reste l'action de scan lorsque l'agent est en mode d'évaluation.

Recherche de cookies

Sélectionnez cette option si vous considérez les cookies comme des risques de sécurité potentiels. Lorsqu'elle est sélectionnée, tous les agents gérés par le serveur scannent les cookies pour y rechercher des spywares/graywares pendant le scan manuel, programmé, en temps réel et immédiat.

Section des paramètres de scan programmé

Seuls les agents configurés pour exécuter le scan programmé utiliseront les paramètres ci-dessous. Le scan programmé peut rechercher les virus/programmes malveillants et les spywares/graywares.

La section Paramètres de scan programmé des paramètres de scan généraux permet aux administrateurs de configurer ce qui suit :

- *Rappeler le scan programmé aux utilisateurs __ minutes avant qu'il ne débute à la page 7-80*
- *Différer le scan programmé de __ heure(s) et __ minute(s) maximum à la page 7-80*

- *Arrêter automatiquement le scan programmé lorsque le scan dure depuis plus de __ heure(s) et __ minute(s) à la page 7-81*
- *Ignorer le scan programmé lorsque l'autonomie de la batterie d'un endpoint sans fil est inférieure à __ % et que son adaptateur secteur est débranché à la page 7-81*
- *Reprendre un scan programmé ignoré à la page 7-81*

Rappeler le scan programmé aux utilisateurs __ minutes avant qu'il ne débute

OfficeScan affiche un message de notification quelques minutes avant que le scan ne débute pour rappeler aux utilisateurs la programmation de scan (date et heure) et tous les privilèges de scan programmé que vous leur avez accordés.

Le message de notification peut être activé/désactivé depuis **Agents** > **Gestion des agents > Paramètres** > **Privilèges et autres paramètres** > **Autres paramètres (onglet)** > **Paramètres de scan programmé**. S'il est désactivé, aucun rappel ne s'affiche.

Différer le scan programmé de __ heure(s) et __ minute(s) maximum

Seuls les utilisateurs disposant du privilège « Différer le scan programmé » peuvent effectuer les actions suivantes :

- Différer le scan programmé avant qu'il ne débute et définir la durée du report.
- Lorsque le scan programmé est en cours, les utilisateurs peuvent l'arrêter et le redémarrer ultérieurement. Les utilisateurs définissent alors la durée devant s'écouler avant le redémarrage du scan. Lorsque le scan reprend, tous les fichiers scannés précédemment sont à nouveau scannés.

  La durée de report maximale/le temps écoulé maximal que les utilisateurs peuvent définir est de 12 heures et 45 minutes. Vous pouvez réduire cette durée en spécifiant le nombre d'heures et/ou de minutes dans les champs prévus à cet effet.

Arrêter automatiquement le scan programmé lorsque le scan dure depuis plus de __ heure(s) et __ minute(s)

OfficeScan arrête le scan lorsque le délai spécifié est dépassé et que le scan n'est pas encore terminé. OfficeScan avertit immédiatement les utilisateurs des risques de sécurité détectés pendant le scan.

Ignorer le scan programmé lorsque l'autonomie de la batterie d'un endpoint sans fil est inférieure à __ % et que son adaptateur secteur est débranché

OfficeScan ignore automatiquement le scan programmé lors de son lancement s'il détecte que l'autonomie de la batterie d'un endpoint sans fil est faible et que son adaptateur secteur n'est pas raccordé à une source d'alimentation. Si l'autonomie de la batterie est faible mais que l'adaptateur CA est raccordé à une source d'alimentation, le scan se poursuit.

Reprendre un scan programmé ignoré

Lorsqu'un scan programmé n'est pas lancé parce que OfficeScan n'est pas en cours d'exécution au jour et à l'heure prévus, vous pouvez indiquer à quel moment OfficeScan reprendra le scan :

- **À la même heure le jour suivant** : si OfficeScan est en cours d'exécution exactement à la même heure le jour suivant, le scan reprend.
- **__ minutes après le démarrage du endpoint** : OfficeScan reprend le scan un certain nombre de minutes après la mise sous tension du endpoint par l'utilisateur. Le nombre de minutes peut être compris entre 10 et 120.



Remarque

Les utilisateurs peuvent reporter ou ignorer un scan programmé repris si l'administrateur leur a accordé ce privilège. Pour obtenir des informations détaillées, voir *Privilèges et autres paramètres de scan programmé à la page 7-59*.

Section des paramètres de bande passante des journaux de virus/programmes malveillants

La section des paramètres de bande passante des journaux de virus/programmes malveillants des paramètres de scan généraux permet aux administrateurs de configurer :

Permettre aux agents OfficeScan de créer une entrée unique dans le journal des virus/programmes malveillants pour les détections récurrentes d'un même virus/programme malveillant en l'espace d'une heure à la page 7-82

Permettre aux agents OfficeScan de créer une entrée unique dans le journal des virus/programmes malveillants pour les détections récurrentes d'un même virus/programme malveillant en l'espace d'une heure

OfficeScan rassemble les entrées des journaux de virus lorsque de multiples infections provenant des mêmes virus/programmes malveillants sont détectées sur une courte période. OfficeScan peut détecter un même virus/programme malveillant à plusieurs reprises. Il remplit alors rapidement le journal des virus/programmes malveillants et sollicite la bande passante du réseau lorsque l'agent OfficeScan envoie les informations du journal au serveur. L'activation de cette fonctionnalité permet de réduire à la fois le nombre d'entrées de virus/programmes malveillants consignées et la bande passante du réseau que les agents OfficeScan utilisent lorsqu'ils soumettent au serveur des informations du journal de virus.

Section consacrée à Certified Safe Software Services

La section **Certified Safe Software Services** qui se trouve sous **Paramètres de scan généraux** permet aux administrateurs de configurer :

Activer Certified Safe Software Service pour la surveillance des comportements, le pare-feu et les scans antivirus à la page 7-83

Activer Certified Safe Software Service pour la surveillance des comportements, le pare-feu et les scans antivirus

Certified Safe Software Service interroge les centres de données Trend Micro pour vérifier la sécurité d'un programme détecté par le blocage du comportement des programmes malveillants, la surveillance des événements, le pare-feu ou les scans antivirus. Activez le service Certified Safe Software Service pour réduire la probabilité de détection de faux-positifs.



Remarque

Vérifiez que les agents OfficeScan disposent des paramètres proxy corrects (pour plus d'informations, voir *Paramètres proxy des agents OfficeScan à la page 14-51*) avant d'activer Certified Safe Software Service. Des paramètres proxy incorrects, de même qu'une connexion Internet intermittente, peuvent entraîner des retards ou un échec de réception d'une réponse des centres de données Trend Micro, et faire que des programmes apparaissent comme sans réponse.

De plus, les agents OfficeScan IPv6 purs ne peuvent pas interroger directement les centres de données Trend Micro. Un serveur proxy à double pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre aux agents OfficeScan de se connecter aux centres de données Trend Micro.

Notifications sur les risques liés à la sécurité

OfficeScan est fourni avec un ensemble de messages de notification par défaut vous informant, ainsi que d'autres administrateurs OfficeScan et les utilisateurs de l'agent OfficeScan, des risques de sécurité détectés.

Pour plus de détails sur les notifications envoyées aux administrateurs, voir *Notifications sur les risques liés à la sécurité pour les administrateurs à la page 7-84*.

Pour plus d'informations sur les notifications envoyées aux utilisateurs des agents OfficeScan, voir *Notifications sur les risques de sécurité pour les utilisateurs des agents OfficeScan à la page 7-88*.

Notifications sur les risques liés à la sécurité pour les administrateurs

Configurez OfficeScan pour qu'il vous envoie, ainsi qu'aux autres administrateurs OfficeScan, une notification lorsqu'un risque lié à la sécurité est détecté ou uniquement lorsque l'action entreprise contre le risque échoue et que par conséquent, une intervention de votre part s'impose.

OfficeScan est fourni avec un ensemble de messages de notification par défaut vous informant, ainsi que les autres administrateurs OfficeScan, des détections de risques liés à la sécurité. Vous pouvez modifier les notifications et configurer des paramètres de notification supplémentaires qui répondent à vos exigences.

Tableau 7-20. Types de notifications de risques de sécurité

Type	Référence
Virus/programmes malveillants	*Configuration des notifications sur les risques liés à la sécurité pour les administrateurs à la page 7-85*
Spyware/Grayware	*Configuration des notifications sur les risques liés à la sécurité pour les administrateurs à la page 7-85*
Transmissions des actifs numériques	*Configuration de la notification de prévention contre la perte de données pour les administrateurs à la page 10-53*
Rappels C&C	*Configuration des notifications sur les rappels C&C pour les administrateurs à la page 11-19*



Remarque

OfficeScan peut envoyer des notifications par courrier électronique, déroutement SNMP et via les journaux d'événements de Windows NT. Configurez les paramètres lorsqu'OfficeScan envoie des notifications par le biais de ces chaînes. Pour obtenir des informations détaillées, voir *Paramètres de notification aux administrateurs à la page 13-33*.

Configuration des notifications sur les risques liés à la sécurité pour les administrateurs

Procédure

1. Accédez à **Administration** > **Notifications** > **Administrateur**.
2. Dans l'onglet **Critères** :
   a. Accédez aux sections **Virus/Programmes malveillants** et **Spywares/Graywares**.
   b. Déterminez si des notifications doivent être envoyées lorsqu'OfficeScan détecte des virus/programmes malveillants et des spywares/graywares ou uniquement lorsque l'action effectuée sur ces risques de sécurité échoue.
3. Dans l'onglet **Courrier électronique** :
   a. Accédez aux sections **Détections de virus/programmes malveillants** et **Détections de spywares/graywares**.
   b. Sélectionnez **Activer la notification par courrier électronique**.
   c. Sélectionnez **Envoyer des notifications aux utilisateurs disposant de droits d'accès aux domaines de l'arborescence des agents**.

      Vous pouvez utiliser l'administration basée sur les rôles afin de donner aux utilisateurs l'accès aux domaines de l'arborescence des agents. Si une anomalie est détectée su un agent OfficeScan appartenant à un domaine spécifique, le courrier électronique sera envoyé aux adresses électroniques des utilisateurs disposant d'autorisations sur ce domaine. Pour des exemples, voir le tableau suivant :

TABLEAU 7-21. Domaines et autorisations de l'arborescence des agents

DOMAINE DE L'ARBORESCENCE DES AGENTS	RÔLES AVEC DROITS D'ACCÈS AU DOMAINE	COMPTE UTILISATEUR AVEC LE RÔLE	ADRESSE ÉLECTRONIQUE POUR LE COMPTE UTILISATEUR
Domaine A	Administrateur (intégré)	racine	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
Domaine B	Administrateur (intégré)	racine	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

Si un agent OfficeScan appartenant au domaine A détecte un virus, le courrier électronique sera envoyé à mary@xyz.com, john@xyz.com et chris@xyz.com.

Si un agent OfficeScan appartenant au domaine B détecte des spywares, le courrier électronique sera envoyé à mary@xyz.com et jane@xyz.com.



Remarque

Si vous activez cette option, tous les utilisateurs ayant les autorisations sur ce domaine doivent avoir des adresses électroniques correspondantes. La notification par courrier électronique ne sera pas envoyée aux utilisateurs qui n'ont pas d'adresse électronique. Les utilisateurs et les adresses électroniques sont configurés à partir de **Administration** > **Gestion des comptes** > **Comptes utilisateurs**.

d. Sélectionnez **Envoyer les notifications à/aux (l')adresse(s) électronique(s) suivante(s)**, puis saisissez les adresses électroniques.

e. Acceptez ou modifiez l'objet et le message par défaut. Vous pouvez utiliser des variables de jeton afin de représenter les données dans les champs **Objet** et **Message**.

Tableau 7-22. Variables de jetons pour les notifications de risques de sécurité

Variable	Description
Détections de virus/programmes malveillants	
%v	Nom du virus/programme malveillant
%s	Endpoint sur lequel se trouve un virus/programme malveillant
%i	Adresse IP du endpoint
%c	Adresse MAC du endpoint
%m	Domaine du endpoint
%p	Emplacement du virus/programme malveillant
%y	Date et heure de la détection du virus/programme malveillant
%e	Version du moteur de scan antivirus
%r	Version du fichier de signatures de virus
%a	Action effectuée sur le risque de sécurité
%n	Nom de l'utilisateur connecté au endpoint infecté
Détections de spywares/graywares	
%s	Endpoint sur lequel se trouve un spyware/grayware
%i	Adresse IP du endpoint
%m	Domaine du endpoint
%y	Date et heure de la détection du spyware/grayware
%n	Nom de l'utilisateur connecté au endpoint au moment de la détection
%T	Résultat de scan anti-spywares/graywares

4. Dans l'onglet **Déroutement SNMP**.

a. Accédez aux sections **Détections de virus/programmes malveillants** et **Détections de spywares/graywares**.

b. Sélectionnez **Activer la notification par déroutement SNMP**.

c. Acceptez ou modifiez le message par défaut. Vous pouvez utiliser des variables de jeton afin de représenter les données dans le champ **Message**. Voir *Tableau 7-22: Variables de jetons pour les notifications de risques de sécurité à la page 7-87* pour plus d'informations.

5. Dans l'onglet **Journal des événements NT** :

a. Accédez aux sections **Détections de virus/programmes malveillants** et **Détections de spywares/graywares**.

b. Sélectionnez **Activer la notification via le journal d'événements NT**.

c. Acceptez ou modifiez le message par défaut. Vous pouvez utiliser des variables de jeton afin de représenter les données dans le champ **Message**. Voir *Tableau 7-22: Variables de jetons pour les notifications de risques de sécurité à la page 7-87* pour plus d'informations.

6. Cliquez sur **Enregistrer**.

Notifications sur les risques de sécurité pour les utilisateurs des agents OfficeScan

OfficeScan peut afficher des messages de notification sur les endpoints des agents OfficeScan :

- Tout de suite après, les scan en temps réel et scan programmé détectent les virus/programmes malveillants et les spywares/graywares. Activez le message de notification et modifiez éventuellement son contenu.
- Si le redémarrage du endpoint d'un agent est nécessaire pour terminer le nettoyage des fichiers infectés. Pour le scan en temps réel, le message s'affiche après la détection d'un risque de sécurité particulier. Pour le scan manuel, le scan programmé et le scan immédiat, le message s'affiche une seule fois, et uniquement après qu'OfficeScan a fini de scanner toutes les cibles de scan.

TABLEAU 7-23. Types de notifications de risques de sécurité pour les agents

TYPE	RÉFÉRENCE
Virus/programmes malveillants	*Configuration des notifications de virus/programme malveillant à la page 7-90*
Spyware/Grayware	*Configuration des notifications de spyware/grayware à la page 7-91*
Violations du pare-feu	*Modification du contenu du message de notification de pare-feu à la page 12-30*
Violations de la réputation de sites Web	*Modification des notifications sur les menaces Internet à la page 11-18*
Violations du contrôle des dispositifs	*Modification des notifications du contrôle des dispositifs à la page 9-18*
Violations de la stratégie de surveillance des comportements	*Modification du contenu du message de notification à la page 8-15*
Transmissions des actifs numériques	*Configuration de la notification de prévention contre la perte de données pour les agents à la page 10-56*
Rappels C&C	*Modification des notifications sur les menaces Internet à la page 11-18*

Notification aux utilisateurs de détections de virus/ programmes malveillants et de spywares/graywares

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Paramètres de scan** > **Paramètres de scan en temps réel** ou **Paramètres** > **Paramètres de scan** > **Paramètres de scan programmé**.

4. Cliquez sur l'onglet **Action**.
5. Sélectionnez les options suivantes :
   - **Afficher un message de notification sur le endpoint de l'agent lorsqu'un virus/programme malveillant est détecté**
   - **Afficher un message de notification sur le endpoint de l'agent lorsqu'un virus/programme malveillant probable est détecté**
6. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :
   - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Configuration des notifications de virus/programme malveillant

---

Procédure

1. Accédez à **Administration** > **Notifications** > **Agent**.
2. Dans la liste déroulante **Type**, sélectionnez **Virus/Programmes malveillants**.
3. Configurez les paramètres de détection.
   a. Choisissez d'afficher une notification pour tous les événements liés aux virus/programmes malveillants ou séparez les notifications en fonction des niveaux de gravité suivants :

- **Élevé** : L'agent OfficeScan n'a pas pu traiter un programme malveillant critique
- **Moyen** : L'agent OfficeScan n'a pas pu traiter un programme malveillant
- **Faible** : L'agent OfficeScan est parvenu à résoudre toutes les menaces

b. Acceptez ou modifiez les messages par défaut.

4. Cliquez sur **Enregistrer**.

Configuration des notifications de spyware/grayware

Procédure

1. Accédez à **Administration** > **Notifications** > **Agent**.
2. Dans la liste déroulante **Type**, sélectionnez **Spywares/Graywares**.
3. Acceptez ou modifiez le message par défaut.
4. Cliquez sur **Enregistrer**.

Notification de redémarrage destinée aux agents afin de terminer le nettoyage de fichiers infectés

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Cliquez sur l'onglet **Autres paramètres** et allez à la section **Notification de redémarrage**.

5. Sélectionnez **Afficher un message de notification si le endpoint doit redémarrer pour terminer le nettoyage des fichiers infectés**.

6. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :

    - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.

    - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Journaux de risques de sécurité

OfficeScan génère des journaux lorsqu'il détecte des virus/programmes malveillants ou des spywares/graywares, et lorsqu'il restaure des spywares/graywares.

Pour éviter que les journaux n'occupent trop d'espace sur votre disque dur, vous pouvez les supprimer manuellement ou configurer leur suppression programmée. Voir *Gestion du journal à la page 13-36* pour obtenir des informations complémentaires sur la gestion des journaux.

Affichage des journaux de virus/programmes malveillants

L'agent OfficeScan génère des journaux lorsqu'il détecte des virus et des programmes malveillants, et envoie ces journaux au serveur.

Procédure

1. Accédez à l'un des emplacements suivants :

    - **Journaux** > **Agents** > **Risques de sécurité**

- **Agents** > **Gestion des agents**

2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.

3. Cliquez sur **Journaux** > **Journaux de virus/programmes malveillants** ou **Afficher journaux** > **Journaux de virus/programmes malveillants**.

4. Spécifiez les critères de journaux, puis cliquez sur **Afficher les journaux**.

5. Affichez les journaux. Les journaux contiennent les informations suivantes :

    - Date et heure de la détection du virus/programme malveillant
    - Endpoint
    - Menace de sécurité
    - Source de l'infection
    - Fichier ou objet infecté
    - Type de scan qui a détecté le virus/programme malveillant
    - Résultats de scan

    Remarque

    Pour plus d'informations sur les résultats de scan, consultez *Résultats de scan antivirus/programmes malveillants à la page 7-94*.

    - adresse IP
    - Adresse MAC
    - Détails des journaux (Cliquez sur **Afficher** pour consulter les détails.)

6. Pour sauvegarder les journaux dans un fichier CSV (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

    Le fichier CSV contient les informations suivantes :

    - Toutes les informations dans les journaux

- Nom de l'utilisateur connecté au endpoint au moment de la détection

Résultats de scan antivirus/programmes malveillants

Les résultats de scan suivants s'affichent dans les journaux de virus/programmes malveillants :

TABLEAU 7-24. Résultats de scan

RÉSULTAT	DESCRIPTION
Supprimé	• La première action est « Supprimer » et le fichier infecté a été supprimé. • La première action est « Nettoyer », mais le nettoyage a échoué. La deuxième action est « Supprimer » et le fichier infecté a été supprimé.« »
Mis en quarantaine	• La première action est « Mettre en quarantaine » et le fichier infecté a été mis en quarantaine. • La première action est « Nettoyer », mais le nettoyage a échoué. La deuxième action est « Mettre en quarantaine » et le fichier infecté a été mis en quarantaine.« »
Nettoyé	Un fichier infecté a été nettoyé.
Renommé	• La première action est « Renommer » et le fichier infecté a été renommé. • La première action est « Nettoyer », mais le nettoyage a échoué. La deuxième action est « Renommer » et le fichier infecté a été renommé.« »
Accès refusé	• La première action est « Refuser l'accès » et l'accès au fichier infecté a été refusé lorsque l'utilisateur a tenté d'ouvrir le fichier. • La première action est « Nettoyer », mais le nettoyage a échoué. La deuxième action est « Refuser l'accès » et l'accès au fichier infecté a été refusé lorsque l'utilisateur a tenté de l'ouvrir.« » • Un virus/programme malveillant potentiel a été détecté lors du scan en temps réel.

RÉSULTAT	DESCRIPTION
	• Le scan en temps réel peut refuser l'accès aux fichiers infectés par un virus d'amorce, même si l'action de scan est « Nettoyer » (première action) et « Mettre en quarantaine » (deuxième action).« »« » Cela est dû au fait que la tentative de nettoyage d'un virus d'amorce risque d'endommager le Master Boot Record (MBR) du endpoint infecté. lancez le scan manuel de sorte qu'OfficeScan puisse nettoyer ou mettre en quarantaine le fichier.
Ignoré	• La première action est « Ignorer ». OfficeScan n'a entrepris aucune action à l'encontre de ce fichier. • La première action est « Nettoyer », mais le nettoyage a échoué. La deuxième action est « Ignorer ». Ainsi, OfficeScan n'a entrepris aucune action à l'encontre du fichier infecté.
Un risque de sécurité potentiel a été ignoré	Ce résultat de scan ne s'affiche que lorsqu'OfficeScan détecte un «virus/programme malveillant potentiel» lors du scan manuel, du scan programmé et du scan immédiat. Reportez-vous à la page suivante de l'encyclopédie en ligne des virus de Trend Micro pour obtenir des informations sur les virus/programmes malveillants potentiels et sur l'envoi de fichiers suspects à Trend Micro pour analyse. http://www.trendmicro.com/vinfo/fr/virusencyclo/default5.asp?VName=POSSIBLE_VIRUS&VSect=Sn
Impossible de nettoyer le fichier ou de le mettre en quarantaine	« Nettoyer » est la première action.« » « Mettre en quarantaine » est la seconde action et les deux actions ont échoué.« » Solution : Voir *Impossible de mettre le fichier en quarantaine/ Impossible de renommer le fichier à la page 7-96*.
Impossible de nettoyer ou supprimer le fichier	« Nettoyer » est la première action.« » « Supprimer » est la seconde action et les deux actions ont échoué.« » Solution : Voir *Impossible de supprimer le fichier à la page 7-96*.
Impossible de nettoyer ou renommer le fichier	« Nettoyer » est la première action.« » « Renommer » est la seconde action et les deux actions ont échoué.« » Solution : Voir *Impossible de mettre le fichier en quarantaine/ Impossible de renommer le fichier à la page 7-96*.

Résultat	Description
Impossible de mettre le fichier en quarantaine/ Impossible de renommer le fichier	Explication 1 Le fichier infecté est peut-être verrouillé par une autre application, est en cours d'exécution ou se trouve sur un CD. OfficeScan mettra en quarantaine/renommera le fichier une fois que l'application aura terminé de traiter le fichier ou après son exécution. Solution Concernant les fichiers infectés sur un CD, Trend Micro déconseille l'utilisation de CD car le virus risque d'infecter les autres ordinateurs du réseau.
	Explication 2 Le fichier infecté se trouve dans le dossier Temporary Internet Files du endpoint de l'agent. Étant donné que le endpoint télécharge des fichiers pendant que vous naviguez, le navigateur Web a peut-être verrouillé le fichier infecté. Après que le navigateur Web a terminé le traitement du fichier, OfficeScan met en quarantaine/renomme le fichier. Solution : Aucune
Impossible de supprimer le fichier	Explication 1 Le fichier infecté est peut-être contenu dans un fichier compressé et le paramètre **Nettoyer/supprimer les fichiers infectés dans les fichiers compressés** sous **Agents** > **Paramètres de l'agent général** est désactivé. Solution Activez l'option **Nettoyer/supprimer les fichiers infectés dans les fichiers compressés**. Lorsqu'il est activé, OfficeScan décompresse le fichier compressé, nettoie/supprime les fichiers infectés contenus dans le fichier compressé, puis le compresse à nouveau.

RÉSULTAT	DESCRIPTION
	Remarque L'activation de ce paramètre est susceptible d'augmenter l'utilisation des ressources du endpoint pendant le scan qui peut, de ce fait, durer plus longtemps.
	Explication 2 Le fichier infecté est peut-être verrouillé par une autre application, est en cours d'exécution ou se trouve sur un CD. OfficeScan renommera le fichier une fois que l'application aura terminé de traiter le fichier ou après son exécution. Solution Concernant les fichiers infectés sur un CD, Trend Micro déconseille l'utilisation de CD car le virus risque d'infecter les autres ordinateurs du réseau.
	Explication 3 Le fichier infecté se trouve dans le dossier Temporary Internet Files du endpoint de l'agent OfficeScan. Étant donné que le endpoint télécharge des fichiers pendant que vous naviguez, le navigateur Web a peut-être verrouillé le fichier infecté. Après que le navigateur web a terminé le traitement du fichier, OfficeScan procède à sa suppression. Solution : Aucune
Impossible d'envoyer le fichier à mettre en quarantaine dans le dossier de quarantaine spécifié	Bien qu'OfficeScan ait correctement mis en quarantaine un fichier dans le dossier `\Suspect` du endpoint de l'agent OfficeScan, le fichier ne peut pas être envoyé vers le répertoire de quarantaine indiqué. Solution Déterminez quel type de scan (manuel, en temps réel, programmé ou immédiat) a détecté le virus/programme malveillant, puis examinez le contenu du répertoire de quarantaine spécifié dans l'onglet **Agents** > **Gestion des agents > Paramètres** > **{Type de scan}** > **Action**.

RÉSULTAT	DESCRIPTION
	Si le répertoire de quarantaine se trouve sur l'ordinateur du serveur OfficeScan ou sur un autre ordinateur du serveur OfficeScan : 1. Vérifiez que l'agent peut se connecter au serveur. 2. Si vous utilisez un répertoire de quarantaine au format URL : a. Assurez-vous que le nom de l'endpoint que vous spécifiez après `http://` est correct. b. Vérifiez la taille du fichier infecté. Si elle excède la taille de fichier maximale spécifiée dans **Administration** > **Paramètres** > **Gestionnaire de quarantaine**, ajustez le paramètre pour l'adapter au fichier. Vous pouvez également effectuer d'autres actions, comme la suppression du fichier. c. Vérifiez la taille du dossier de quarantaine et déterminez si celui-ci a dépassé la capacité spécifiée dans **Administration** > **Paramètres** > **Gestionnaire de quarantaine**. Ajustez la capacité du dossier ou supprimez manuellement les fichiers du répertoire de quarantaine. 3. Si vous utilisez un chemin UNC, vérifiez que le répertoire de quarantaine est partagé avec le groupe « Tous » et que vous avez attribué des autorisations en lecture et en écriture à ce groupe.« » Vérifiez également que le répertoire de quarantaine existe et que le chemin UNC est correct. Si le répertoire de quarantaine se trouve sur un autre endpoint du réseau (vous ne pouvez utiliser qu'un chemin UNC pour ce scénario) : 1. Vérifiez que l'agent OfficeScan peut se connecter au endpoint. 2. Vérifiez que le répertoire de quarantaine est partagé avec le groupe « Tous » et que vous avez attribué des autorisations en lecture et en écriture à ce groupe.« » 3. Vérifiez que le répertoire de quarantaine existe. 4. Vérifiez que le chemin UNC est correct. Si le répertoire de quarantaine se trouve dans un répertoire différent du endpoint de l'agent OfficeScan (vous ne pouvez

RÉSULTAT	DESCRIPTION
	utiliser qu'un chemin absolu pour ce scénario), vérifiez que le répertoire de quarantaine existe.
Impossible de nettoyer le fichier	Explication 1 Le fichier infecté peut être contenu dans un fichier compressé et le paramètre « Nettoyer/Supprimer » les fichiers infectés dans les fichiers compressés sous **Agents** > **Paramètres de l'agent général** est désactivé.« » Solution Activez l'option **Nettoyer/supprimer les fichiers infectés dans les fichiers compressés**. Lorsqu'il est activé, OfficeScan décompresse le fichier compressé, nettoie/supprime les fichiers infectés contenus dans le fichier compressé, puis le compresse à nouveau. **Remarque** L'activation de ce paramètre est susceptible d'augmenter l'utilisation des ressources du endpoint pendant le scan qui peut, de ce fait, durer plus longtemps.
	Explication 2 Le fichier infecté se trouve dans le dossier `Temporary Internet Files` du endpoint de l'agent OfficeScan. Étant donné que le endpoint télécharge des fichiers pendant que vous naviguez, le navigateur Web a peut-être verrouillé le fichier infecté. Après que le navigateur Web a terminé le traitement du fichier, OfficeScan procède à son nettoyage. Solution : Aucune
	Explication 3 Il se peut que le fichier ne puisse pas être nettoyé. Pour plus de détails et connaître les solutions, reportez-vous à *Fichiers non nettoyables à la page E-17*.
Action requise	OfficeScan ne parvient pas à effectuer l'action configurée sur le fichier infecté sans intervention de l'utilisateur. Passez votre

RÉSULTAT	DESCRIPTION
	souris sur la colonne **Action requise** pour afficher les détails suivants : • « Action requise - Contactez l'assistance pour obtenir des détails sur la façon de supprimer cette menace à l'aide de l'outil « Clean Boot » de l'Anti-Threat Tool Kit, qui se trouve dans la boîte à outils OfficeScan » • « Action requise - Contactez l'assistance pour obtenir des détails sur la façon de supprimer cette menace à l'aide de l'outil « Rescue Disk » de l'Anti-Threat Tool Kit, qui se trouve dans la boîte à outils OfficeScan » • « Action requise - Contactez l'assistance pour obtenir des détails sur la façon de supprimer cette menace à l'aide de l'outil « Rootkit Buster » de l'Anti-Threat Tool Kit, qui se trouve dans la boîte à outils OfficeScan » • « Action requise - OfficeScan a détecté une menace sur un agent infecté. Redémarrez le endpoint pour terminer le nettoyage de la menace de sécurité » • « Action requise - Effectuez un scan système complet »

Affichage des journaux de restauration depuis la mise en quarantaine centrale

Après avoir nettoyé des programmes malveillants, les agents OfficeScan sauvegardent les données les concernant. Demandez aux agents en ligne de restaurer les données sauvegardées si vous considérez que les données sont inoffensives. Les informations relatives aux données de sauvegarde des programmes malveillants restaurées, au endpoint concerné et au résultat de la restauration sont disponibles dans les journaux.

Procédure

1. Accédez à **Journaux** > **Agents** > **Restauration depuis la mise en quarantaine centrale**.

2. Consultez les colonnes **Réussi**, **Échoué** et **En attente** pour savoir si OfficeScan est parvenu à restaurer les données mises en quarantaine.

3. Cliquez sur les liens numérotés de chaque colonne pour afficher des informations détaillées sur chaque endpoint affecté.



Remarque

Pour les restaurations ayant **Échoué**, vous pouvez lancer une nouvelle tentative de restauration du fichier sur l'écran **Détails de la restauration depuis la mise en quarantaine centrale**, en cliquant sur **Tout restaurer**.

4. Pour sauvegarder les journaux dans un fichier CSV (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Affichage des journaux de spywares/graywares

L'agent OfficeScan génère des journaux lorsqu'il détecte des spywares et graywares, et envoie ces journaux au serveur.

Procédure

1. Accédez à l'un des emplacements suivants :
   - **Journaux** > **Agents** > **Risques de sécurité**
   - **Agents** > **Gestion des agents**
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Journaux** > **Journaux de spywares/graywares** ou **Afficher journaux** > **Journaux de spywares/graywares**.
4. Spécifiez les critères de journaux, puis cliquez sur **Afficher les journaux**.
5. Affichez les journaux. Les journaux contiennent les informations suivantes :
   - Date et heure de la détection du spyware/grayware
   - Endpoint affecté

- Nom du spyware/grayware
- Type de scan qui a détecté le spyware/grayware
- Détails sur les résultats de scan anti-spywares/graywares (si l'action de scan a réussi ou non). Voir *Résultats de scan anti-spywares/graywares à la page 7-102* pour obtenir des informations détaillées.
- adresse IP
- Adresse MAC
- Détails des journaux (Cliquez sur **Afficher** pour consulter les détails.)

6. Ajoutez les spywares/graywares que vous considérez inoffensifs à la Liste des spywares/graywares approuvés.
7. Pour sauvegarder les journaux dans un fichier CSV (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

   Le fichier CSV contient les informations suivantes :

   - Toutes les informations dans les journaux
   - Nom de l'utilisateur connecté au endpoint au moment de la détection

Résultats de scan anti-spywares/graywares

Les résultats de scan suivants s'affichent dans les journaux de spywares/graywares :

TABLEAU 7-25. Résultats de scan anti-spywares/graywares de premier niveau

RÉSULTAT	DESCRIPTION
Réussite. Aucune autre action requise	Il s'agit du résultat de premier niveau si le scan est une réussite. Le résultat de deuxième niveau peut être l'un des suivants : • *Nettoyé* • *Accès refusé*

RÉSULTAT	DESCRIPTION
Action supplémentaire requise	Il s'agit du résultat de premier niveau si le scan est un échec. Les résultats du deuxième niveau contiennent au moins l'un des messages suivants : • *Ignoré* • *Spywares/graywares dangereux à nettoyer.* • *Scan anti-spywares/graywares arrêté manuellement. Veuillez effectuer un scan complet* • *Spyware/grayware nettoyé, redémarrage requis. Redémarrez l'ordinateur* • *Impossible de nettoyer les spywares/graywares* • *Résultat de scan anti-spywares/graywares inconnu. Contactez l'assistance technique de Trend Micro*

TABLEAU 7-26. Résultats de scan anti-spywares/graywares de second niveau

RÉSULTAT	DESCRIPTION	SOLUTION
Nettoyé	OfficeScan a mis fin aux processus ou supprimé les registres, fichiers, cookies et raccourcis.	N/A
Accès refusé	OfficeScan a refusé l'accès (copie, ouverture) aux composants de spyware/ grayware détectés.	N/A
Ignoré	OfficeScan n'a entrepris aucune action mais a consigné la détection de spyware/ grayware pour évaluation.	ajoutez les spywares/ graywares que vous considérez sans danger à la liste des spywares/ graywares approuvés.

Résultat	Description	Solution
Spywares/ graywares dangereux à nettoyer.	: ce message s'affiche si le moteur de scan anti-spywares tente de nettoyer un dossier unique et si les critères suivants sont remplis : • Les éléments à nettoyer dépassent 250 Mo. • Le système d'exploitation utilise les fichiers dans le dossier. Le dossier est également nécessaire pour le bon fonctionnement du système. • Le dossier est un répertoire racine (tel que `C:` ou `F:`)	Contactez le service d'assistance pour obtenir de l'aide.
Scan anti-spywares/ graywares arrêté manuellement. Veuillez effectuer un scan complet	un utilisateur a interrompu un scan avant qu'il soit achevé.	exécutez un scan manuel et attendez que le scan soit achevé.
Spyware/grayware nettoyé, redémarrage requis. Redémarrez l'ordinateur	OfficeScan a nettoyé des composants de spyware/grayware mais un redémarrage du endpoint est requis pour terminer la tâche.	Redémarrez le endpoint immédiatement.
Impossible de nettoyer les spywares/ graywares	Un spyware/Grayware a été détecté sur un CD-ROM ou sur un lecteur de réseau. OfficeScan ne peut pas nettoyer les spywares/graywares détectés à ces emplacements.	Supprimez manuellement le fichier infecté.
Résultat de scan anti-spywares/ graywares inconnu. Contactez l'assistance technique de Trend Micro	Une nouvelle version du moteur de scan anti-spyware fournit un nouveau résultat de scan que la configuration d'OfficeScan ne permet pas de traiter.	contactez votre service d'assistance pour obtenir de l'aide afin de déterminer le nouveau résultat de scan.

Affichage des journaux de restauration de spywares/ graywares

Après avoir nettoyé les spywares/graywares, les agents OfficeScan sauvegardent les données des spywares/graywares. Demandez aux agents en ligne de restaurer les données sauvegardées si vous considérez que les données sont inoffensives. Les informations relatives aux données de sauvegarde des spywares/graywares restaurées, au endpoint concerné et au résultat de la restauration sont disponibles dans les journaux.

Procédure

1. Accédez à **Journaux** > **Agents** > **Restauration de spywares/graywares**.
2. Consultez la colonne **Résultat** pour vérifiez si OfficeScan a réussi la restauration des données de spywares/graywares.
3. Pour sauvegarder les journaux dans un fichier CSV (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Journaux de scan

Lorsque le scan manuel, le scan programmé ou le scan immédiat s'exécute, l'agent OfficeScan créé un journal de scan contenant des informations sur le scan. Vous pouvez consulter le journal de scan en accédant à la console de l'agent OfficeScan. Les agents n'envoient pas le journal de scan au serveur.

Les journaux de scan présentent les informations suivantes :

- Date et heure à laquelle OfficeScan a commencé le scan
- Date et heure à laquelle OfficeScan a arrêté le scan
- État du scan
    - **Terminé** : Le scan s'est terminé sans problème.
    - **Arrêté** : L'utilisateur a interrompu le scan avant qu'il ne soit achevé.

  - **Arrêté de manière inattendue** : Le scan a été interrompu par l'utilisateur, le système, ou par un événement inattendu. Par exemple, il se peut que le service de scan en temps réel OfficeScan se soit terminé de façon inattendue ou que l'utilisateur ait effectué un redémarrage forcé de l'agent.

- Type de scan
- Nombre d'objets scannés
- Nombre de fichiers infectés
- Nombre d'actions ayant échoué
- Nombre d'actions ayant réussi
- Version de Smart Scan Agent Pattern
- Version du fichier de signatures de virus
- Version du fichier de signatures de spywares

Épidémies de risques liés à la sécurité

Une épidémie de risques se déclare lorsque les détections de virus/programmes malveillants, spywares/graywares et sessions de partage de dossiers dépassent le seuil défini sur une certaine période. Il existe plusieurs manières de répondre et de contenir des épidémies sur le réseau, notamment:

- Activation d'OfficeScan pour surveiller le réseau à la recherche de toute activité suspecte
- Blocage des dossiers et des ports importants des endpoints des agents
- Envoi aux agents de messages d'alerte d'épidémie
- Nettoyage des endpoints infectés

Critères et notifications d'épidémies de risques liés à la sécurité

Configurez OfficeScan afin que vous et les autres administrateurs OfficeScan receviez une notification lorsque l'un des événements suivants survient :

TABLEAU 7-27. Types de notifications d'épidémies de risques de sécurité

TYPE	RÉFÉRENCE
• Virus/programmes malveillants • Spyware/Grayware • Session de partage de dossiers	*Configuration des critères et notifications d'épidémies de risques liés à la sécurité à la page 7-108*
Violations du pare-feu	*Configuration des critères et notifications de l'épidémie de violation du pare-feu à la page 12-32*
Rappels C&C	*Configuration des critères et notifications de l'épidémie de violation des rappels C&C à la page 11-22*

- Épidémie de virus/programmes malveillants
- Épidémie de spywares/graywares
- Épidémies de violation du pare-feu
- Épidémie de sessions de partage de dossiers

Définissez une épidémie selon le nombre de détections et la période de détection. Une épidémie se déclenche lorsque le nombre de détections dépasse le seuil défini au cours de la période de détection.

OfficeScan est fourni avec un ensemble de messages de notification par défaut vous informant, ainsi que les autres administrateurs OfficeScan, d'une épidémie. Vous pouvez modifier les notifications et configurer des paramètres de notification supplémentaires qui répondent à vos exigences.



Remarque

OfficeScan peut envoyer des notifications d'épidémies de risques de sécurité par courrier électronique, déroutement SNMP et via les journaux d'événements de Windows NT. Pour les épidémies de sessions de partage de dossiers, OfficeScan envoie des notifications par e-mail. Configurez les paramètres lorsqu'OfficeScan envoie des notifications par le biais de ces chaînes. Pour obtenir des informations détaillées, voir *Paramètres de notification aux administrateurs à la page 13-33*.

Configuration des critères et notifications d'épidémies de risques liés à la sécurité

Procédure

1. Accédez à **Administration** > **Notifications** > **Épidémie**.
2. Dans l'onglet **Critères** :
    a. Accédez aux sections **Virus/Programmes malveillants** et **Spyware/ Grayware** :
    b. Spécifiez le nombre de sources uniques de détections.
    c. Déterminez le nombre de détections et la période de détection pour chaque risque de sécurité.

    Conseil

    Trend Micro recommande d'accepter les valeurs par défaut dans cet écran.

    OfficeScan envoie un message de notification lorsque le nombre de détections est dépassé. Par exemple, sous la section **Virus/Programmes malveillants**, si vous spécifiez 10 sources uniques, 100 détections et une durée de 5 heures, OfficeScan envoie une notification lorsque 10 agents différents rapportent un nombre total de 101 risques de sécurité sur une période de 5 heures. Si toutes les détections effectuées au cours de la période de 5 heures concernent un seul agent, OfficeScan n'envoie pas de notification.
3. Dans l'onglet **Critères** :

a. Accédez à la section **Sessions de partage de dossiers**.

b. Sélectionnez **Contrôler les sessions de partage de dossiers sur votre réseau**.

c. Sous **Sessions de partage de dossiers enregistrées**, cliquez sur le lien numéroté pour afficher les ordinateurs hébergeant des dossiers partagés et les ordinateurs accédant aux dossiers partagés.

d. Indiquez le nombre de sessions de partage de dossiers ainsi que la période de détection.

OfficeScan envoie un message de notification lorsque le nombre de sessions de partage de dossiers est dépassé.

4. Dans l'onglet **Courrier électronique** :

a. Accédez aux sections **Épidémies de virus/programmes malveillants**, **Épidémies de spywares/graywares** et **Épidémies de sessions de partage de dossiers**.

b. Sélectionnez **Activer la notification par courrier électronique**.

c. Indiquez les destinataires de l'e-mail.

d. Acceptez ou modifiez l'objet et le message par défaut de l'e-mail. Vous pouvez utiliser des variables de jeton afin de représenter les données dans les champs **Objet** et **Message**.

TABLEAU 7-28. Variables de jetons pour les notifications d'épidémies de risques liés à la sécurité

VARIABLE	DESCRIPTION
Épidémies de virus/programmes malveillants	
%CV	Nombre total de virus/programmes malveillants détectés
%CC	Nombre total d'ordinateurs infectés par des virus/programmes malveillants
Épidémies de spywares/graywares	
%CV	Nombre total de spywares/graywares détectés

VARIABLE	DESCRIPTION
%CC	Nombre total d'ordinateurs infectés par des spywares/graywares
Épidémies de sessions de partage de dossiers	
%S	Nombre de sessions de partage de dossiers
%T	Période d'accumulation des sessions de partage de dossiers
%M	Période, exprimée en minutes

e. Sélectionnez des informations supplémentaires sur les virus/programmes malveillants et les spywares/graywares à inclure dans l'e-mail. Vous pouvez inclure le nom de l'agent/domaine, le nom du risque de sécurité, la date et l'heure de la détection, le chemin d'accès et le nom du fichier infecté, ainsi que le résultat du scan.

f. Acceptez ou modifiez les messages de notification par défaut.

5. Dans l'onglet **Déroutement SNMP**.

   a. Accédez aux sections **Épidémies de virus/programmes malveillants** et **Épidémies de spywares/graywares**.

   b. Sélectionnez **Activer la notification par déroutement SNMP**.

   c. Acceptez ou modifiez le message par défaut. Vous pouvez utiliser des variables de jeton afin de représenter les données dans le champ **Message**. Voir *Tableau 7-28: Variables de jetons pour les notifications d'épidémies de risques liés à la sécurité à la page 7-109* pour obtenir des informations détaillées.

6. Dans l'onglet **Journal des événements NT** :

   a. Accédez aux sections **Épidémies de virus/programmes malveillants** et **Épidémies de spywares/graywares**.

   b. Sélectionnez **Activer la notification via le journal d'événements NT**.

   c. Acceptez ou modifiez le message par défaut. Vous pouvez utiliser des variables de jeton afin de représenter les données dans le champ **Message**. Voir *Tableau 7-28: Variables de jetons pour les notifications d'épidémies de risques liés à la sécurité à la page 7-109* pour obtenir des informations détaillées.

7. Cliquez sur **Enregistrer**.

Configuration de la prévention des épidémies de risques liés à la sécurité

Lorsqu'une épidémie se produit, appliquez les mesures de prévention des épidémies pour répondre à l'épidémie et la contenir. Configurez soigneusement les paramètres de prévention car une mauvaise configuration peut entraîner des problèmes de réseau imprévus.

Procédure

1. Accédez à **Agents** > **Prévention des épidémies**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Démarrer la prévention des épidémies**.
4. Cliquez sur l'une des stratégies suivantes de prévention des épidémies, puis configurez les paramètres qui s'y appliquent :
   - *Limitation/interdiction de l'accès aux dossiers partagés à la page 7-113*
   - *Blocage des ports vulnérables à la page 7-114*
   - *Interdiction de l'accès en écriture aux fichiers et dossiers à la page 7-115*
   - *Refus de l'accès aux fichiers compressés exécutables à la page 7-118*
   - *Création d'une règle de traitement par exclusion mutuelle pour les fichiers/processus de programmes malveillants à la page 7-117*
5. Sélectionnez les stratégies à appliquer.
6. Sélectionnez le nombre d'heures pendant lesquelles la prévention des épidémies sera active. La valeur par défaut est fixée à 48 heures. Vous pouvez restaurer manuellement les paramètres du réseau avant l'expiration de la période de prévention des épidémies.



AVERTISSEMENT!

N'autorisez pas l'activation permanente de la prévention des épidémies. Pour bloquer ou refuser l'accès à certains fichiers, dossiers ou ports, modifiez directement les paramètres du endpoint et du réseau au lieu d'utiliser OfficeScan.

7. Acceptez ou modifiez le message de notification de l'agent par défaut.



Remarque

Pour configurer OfficeScan afin qu'il vous envoie une notification en cas d'épidémie, accédez à **Administration** > **Notifications** > **Épidémie**.

8. Cliquez sur **Démarrer la prévention des épidémies**.

   Les mesures de prévention des épidémies que vous avez sélectionnées s'affichent dans une nouvelle fenêtre.

9. De retour dans l'arborescence des agents, observez la colonne **Prévention des épidémies**.

   Une coche apparaît sur les ordinateurs qui appliquent des mesures de prévention des épidémies.

OfficeScan consigne les événements suivants dans les journaux d'événements du système :

- Événements liés aux serveurs (qui lancent le processus de prévention des épidémies et envoient aux agents des notifications leur demandant d'activer cette fonctionnalité)
- Événements liés aux agents OfficeScan (qui activent la prévention des épidémies)

Stratégies de prévention des épidémies

Lorsqu'une épidémie se produit, appliquez l'une des stratégies suivantes :

- *Limitation/interdiction de l'accès aux dossiers partagés à la page 7-113*
- *Blocage des ports vulnérables à la page 7-114*

- *Interdiction de l'accès en écriture aux fichiers et dossiers à la page 7-115*
- *Refus de l'accès aux fichiers compressés exécutables à la page 7-118*
- *Création d'une règle de traitement par exclusion mutuelle pour les fichiers/processus de programmes malveillants à la page 7-117*

Limitation/interdiction de l'accès aux dossiers partagés

Pendant les épidémies, vous pouvez limiter ou interdire l'accès aux dossiers partagés sur le réseau pour empêcher la propagation des risques de sécurité à travers les dossiers partagés.

Lorsque cette stratégie entre en vigueur, les utilisateurs peuvent continuer de partager des dossiers mais elle ne s'applique pas aux dossiers qui viennent d'être partagés. Vous devez donc informer les utilisateurs pour qu'ils ne partagent pas les dossiers au cours d'une épidémie ou déployer de nouveau la stratégie pour l'appliquer aux dossiers qui viennent d'être partagés.

Procédure

1. Accédez à **Agents** > **Prévention des épidémies**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Démarrer la prévention des épidémies**.
4. Cliquez sur **Limitation/interdiction de l'accès aux dossiers partagés**.
5. Sélectionnez l'une des options suivantes :
   - **Autoriser l'accès en lecture seule** limite l'accès aux dossiers partagés
   - **Refuser tout accès**



Remarque

le paramètre d'accès en lecture seule ne s'applique pas aux dossiers partagés déjà configurés pour interdire tout accès.

---

6. Cliquez sur **Enregistrer**.

   L'écran **Paramètres de prévention des épidémies** s'affiche de nouveau.

7. Cliquez sur **Démarrer la prévention des épidémies**.

   Les mesures de prévention des épidémies que vous avez sélectionnées s'affichent dans une nouvelle fenêtre.

Blocage des ports vulnérables

Pendant les épidémies, bloquez les ports vulnérables que les virus/programmes malveillants pourraient exploiter pour accéder aux ordinateurs des agents OfficeScan.



AVERTISSEMENT!

Configurez alors les paramètres de prévention des épidémies avec soin. Le blocage des ports utilisés rendra indisponibles les services réseau qui dépendent de ces ports. Par exemple, si vous bloquez le port sécurisé, OfficeScan ne peut plus communiquer avec l'agent pendant l'épidémie.

Procédure

1. Accédez à **Agents** > **Prévention des épidémies**.

2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.

3. Cliquez sur **Démarrer la prévention des épidémies**.

4. Cliquez sur **Blocage des ports**.

5. Sélectionnez **Bloquer un port sécurisé**.

6. Sélectionnez les ports à bloquer dans la colonne **Ports bloqués**.

   a. Si aucun port ne figure dans le tableau, cliquez sur **Ajouter**. Dans l'écran qui s'affiche, sélectionnez les ports à bloquer puis cliquez sur **Enregistrer**.

- **Tous les ports (y compris ICMP)** : bloque tous les ports sauf le port sécurisé. Pour bloquer également le port sécurisé, cochez la case Bloquer le port sécurisé dans l'écran précédent.
- **Ports fréquemment utilisés** : sélectionnez au moins un numéro de port pour permettre à OfficeScan d'enregistrer les paramètres de blocage des ports.
- **Ports des chevaux de Troie** : bloque les ports habituellement utilisés par les programmes de type Cheval de Troie. Voir *Port des chevaux de Troie à la page E-14* pour obtenir des informations détaillées.
- **Un numéro de port ou une plage de ports** : vous pouvez indiquer de façon facultative la direction du trafic à bloquer et certains commentaires, comme la raison pour laquelle vous bloquez les ports spécifiés.
- **Protocole ping (Rejeter ICMP)** : cliquez sur cette option pour bloquer uniquement les paquets ICMP, tels que les requêtes ping.

b. Pour modifier les paramètres du ou des ports bloqués, cliquez sur le numéro du port.

c. Dans l'écran qui s'affiche, modifiez les paramètres puis cliquez sur **Enregistrer**.

d. Pour supprimer un port de la liste, sélectionnez la case à cocher en regard du numéro de port puis cliquez sur **Supprimer**.

7. Cliquez sur **Enregistrer**.

   L'écran **Paramètres de prévention des épidémies** s'affiche de nouveau.

8. Cliquez sur **Démarrer la prévention des épidémies**.

   Les mesures de prévention des épidémies que vous avez sélectionnées s'affichent dans une nouvelle fenêtre.

Interdiction de l'accès en écriture aux fichiers et dossiers

Les virus/programmes malveillants peuvent modifier ou supprimer les fichiers et les dossiers stockés sur les ordinateurs infectés. En cas d'épidémie, configurez OfficeScan

de telle sorte que les virus/programmes malveillants ne puissent pas modifier ni supprimer des fichiers ni des dossiers des ordinateurs des agents OfficeScan.



AVERTISSEMENT!

OfficeScan ne prend pas en charge l'interdiction du droit en écriture sur des lecteurs réseau mappés.

Procédure

1. Accédez à **Agents** > **Prévention des épidémies**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine (icône) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Démarrer la prévention des épidémies**.
4. Cliquez sur **Interdire l'accès en écriture aux fichiers et dossiers**.
5. Entrez le chemin du répertoire. Lorsque vous aurez saisi le chemin d'accès au répertoire que vous souhaitez protéger, cliquez sur **Ajouter**.

   Remarque

   Saisissez le chemin d'accès absolu au répertoire, et non le chemin d'accès virtuel.

6. Spécifiez les fichiers à protéger dans les répertoires protégés. Sélectionnez tous les fichiers ou uniquement les fichiers avec une extension déterminée. Pour les extensions de fichiers, spécifiez une extension qui ne figure pas dans la liste proposée en la saisissant dans la zone de texte, puis en cliquant sur **Ajouter**.
7. Pour protéger des fichiers spécifiques, sous **Fichiers à protéger**, entrez le nom de fichier complet et cliquez sur **Ajouter**.
8. Cliquez sur **Enregistrer**.

   L'écran **Paramètres de prévention des épidémies** s'affiche de nouveau.

9. Cliquez sur **Démarrer la prévention des épidémies**.

Les mesures de prévention des épidémies que vous avez sélectionnées s'affichent dans une nouvelle fenêtre.

Création d'une règle de traitement par exclusion mutuelle pour les fichiers/processus de programmes malveillants

Vous pouvez configurer la prévention des épidémies afin d'assurer la protection contre les menaces de sécurité qui utilisent des processus mutex en écrasant les ressources requises par la menace pour parvenir à infecter le système et s'y propager. La prévention des épidémies crée des règles d'exclusion mutuelle pour les fichiers et processus associés à des programmes malveillants connus, empêchant ainsi ces programmes malveillants d'accéder à ces ressources.



Conseil

Trend Micro recommande la conservation de ces exclusions jusqu'à la mise en œuvre d'une solution durable contre ces menaces liées à des programmes malveillants. Contactez l'assistance pour obtenir le nom des mutex permettant d'assurer une protection lors d'épidémies.



Remarque

La gestion des exclusions mutuelles requiert le service de prévention des modifications non autorisées et prend uniquement en charge les plates-formes 32 bits.

Procédure

1. Accédez à **Agents** > **Prévention des épidémies**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Démarrer la prévention des épidémies**.
4. Cliquez sur **Créer une règle de traitement par exclusion mutuelle (mutex) pour les fichiers/processus de programmes malveillants**.
5. Saisissez le nom du mutex contre lequel assurer une protection dans la zone de texte prévue à cet effet.

Ajoutez ou supprimez des noms de mutex dans la liste à l'aide des boutons **+** et **-**.



Remarque

La prévention des épidémies prend en charge la gestion des exclusions mutuelles sur un maximum de six menaces mutex.

6. Cliquez sur **Enregistrer**.

   L'écran **Paramètres de prévention des épidémies** s'affiche de nouveau.

7. Cliquez sur **Démarrer la prévention des épidémies**.

   Les mesures de prévention des épidémies que vous avez sélectionnées s'affichent dans une nouvelle fenêtre.

Refus de l'accès aux fichiers compressés exécutables

Lorsqu'une épidémie se déclare, il est préférable de refuser l'accès aux fichiers compressés exécutables afin d'éviter la propagation sur l'ensemble du réseau du risque de sécurité que ces fichiers peuvent potentiellement représenter. Vous pouvez décider d'autoriser l'accès aux fichiers sécurisés créés par les programmes de compression de fichiers exécutables pris en charge.

Procédure

1. Accédez à **Agents** > **Prévention des épidémies**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Démarrer la prévention des épidémies**.
4. Cliquez sur **Refuser l'accès aux fichiers compressés exécutables**.
5. Faites votre choix dans la liste des programmes de compression de fichiers exécutables pris en charge, puis cliquez sur **Ajouter** pour autoriser l'accès aux fichiers compressés exécutables créés par ces programmes.



Remarque

Vous pouvez uniquement approuver l'utilisation des fichiers compressés créés par les programmes de compression qui se trouvent dans la liste. La prévention des épidémies refuse l'accès à tout autre format de fichier compressé exécutable.

6. Cliquez sur **Enregistrer**.

   L'écran **Paramètres de prévention des épidémies** s'affiche de nouveau.

7. Cliquez sur **Démarrer la prévention des épidémies**.

   Les mesures de prévention des épidémies que vous avez sélectionnées s'affichent dans une nouvelle fenêtre.

Désactivation de la prévention des épidémies

Si vous êtes absolument certain que l'épidémie détectée a été contenue et qu'OfficeScan a déjà nettoyé ou mis en quarantaine tous les fichiers infectés, rétablissez les valeurs normales de vos paramètres réseau en désactivant la fonction de prévention des épidémies.

Procédure

1. Accédez à **Agents** > **Prévention des épidémies**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Rétablir les paramètres**.
4. Pour faire savoir aux utilisateurs que l'épidémie est terminée, sélectionnez **Avertir les utilisateurs une fois les paramètres d'origine restaurés**.
5. Acceptez ou modifiez le message de notification de l'agent par défaut.
6. Cliquez sur **Rétablir les paramètres**.



Remarque

Si vous ne restaurez pas les paramètres réseau manuellement, OfficeScan les restaure automatiquement après expiration du nombre d'heures spécifié dans **Restaurer automatiquement les paramètres initiaux du réseau après __ heures** dans l'écran **Paramètres de prévention des épidémies**. La valeur par défaut est fixée à 48 heures.

OfficeScan consigne les événements suivants dans les journaux d'événements du système :

- Événements liés aux serveurs (qui lancent le processus de prévention des épidémies et envoient aux agents OfficeScan des notifications leur demandant d'activer cette fonctionnalité)
- Événements liés aux agents OfficeScan (qui activent la prévention des épidémies)

7. Après avoir désactivé la prévention des épidémies, recherchez les risques liés à la sécurité sur les ordinateurs en réseau pour vous assurer que l'épidémie a été contenue.



Chapitre 8

Utilisation de la surveillance des comportements

Ce chapitre explique comment protéger les ordinateurs des risques de sécurité en utilisant la fonctionnalité de surveillance des comportements.

Les rubriques sont les suivantes :

Surveillance des comportements

La surveillance des comportements surveille continuellement les endpoints, guettant les modifications inhabituelles du système d'exploitation ou des logiciels installés. La surveillance des comportements protège les endpoints via le **blocage du comportement des programmes malveillants** et la **surveillance des événements**. Une **liste d'exceptions** configurée par l'utilisateur et **Certified Safe Software Service** viennent compléter ces deux fonctionnalités.



Important

- La surveillance des comportements ne prend pas en charge les plates-formes 64 bits Windows XP ou Windows 2003.
- La surveillance des comportements prend en charge les plates-formes 64 bits Windows Vista SP1 ou version ultérieure.
- Par défaut, la surveillance des comportements est désactivée pour toutes les versions de Windows Server 2003, Windows Server 2008 et Windows Server 2012. Avant d'activer la surveillance des comportements sur ces plates-formes serveur, consultez les instructions et pratiques recommandées décrites dans *Services de l'agent OfficeScan à la page 14-7*.

Blocage du comportement des programmes malveillants

Le blocage du comportement des programmes malveillants fournit un niveau nécessaire de protection supplémentaire contre les menaces pour les programmes qui affichent un comportement malveillant. Il observe les événements du système sur une période de temps. Pendant que les programmes exécutent différentes combinaisons ou séquences d'actions, le blocage du comportement des programmes malveillants détecte les comportements malveillants connus et bloque les programmes associés. Utilisez cette fonctionnalité pour vous assurer un niveau de protection plus élevé contre les menaces nouvelles, inconnues et émergentes.

La surveillance des comportements des programmes malveillants fournit les options de scan, au niveau des menaces, suivantes :

- **Menaces connues** : bloque les comportements associés à des menaces connues liées à des programmes malveillants

- **Menaces connues et potentielles** : bloque les comportements associés à des menaces connues et entreprend une action sur les comportements potentiellement malveillants

Lorsqu'un programme est bloqué et que les notifications sont activées, OfficeScan affiche une notification sur le endpoint de l'agent OfficeScan. Pour plus de détails sur les notifications, voir *Notifications de surveillance des comportements pour les utilisateurs des agents OfficeScan à la page 8-14*.

Surveillance des événements

La surveillance des événements fournit une approche plus générique de la protection contre les logiciels non autorisés et les attaques de programmes malveillants. Elle surveille les zones du système pour certains événements, permettant aux administrateurs de gérer les programmes qui déclenchent ces événements. Utilisez la surveillance des événements si vous avez des exigences de protection du système spécifiques différentes de la protection fournie par le blocage du comportement des programmes malveillants.

Le tableau suivant répertorie les événements du système surveillés.

TABLEAU 8-1. Événements du système surveillés

ÉVÉNEMENTS	DESCRIPTION
Fichier système dupliqué	Bon nombre de programmes malveillants créent des copies d'eux-mêmes ou d'autres programmes malveillants en se servant de noms de fichiers utilisés par les fichiers système Windows. Ceci a généralement pour but d'écraser ou de remplacer ces fichiers système, d'éviter la détection ou de décourager les utilisateurs de supprimer les programmes malveillants.
Modification du fichier Hosts	Le fichier Hosts établit la correspondance entre les noms de domaine et les adresses IP. De nombreux programmes malveillants modifient le fichier Hosts de telle sorte que le navigateur Web soit redirigé vers des sites Web infectés, inexistants ou contrefaits.
Comportement suspect	Le comportement suspect peut être une action spécifique ou une série d'actions inhabituelles de la part de programmes légitimes. Les programmes présentant un comportement suspect doivent être employés avec la plus grande prudence.

Événements	Description
Nouveau plug-in Internet Explorer	Les programmes malveillants de type spywares/graywares installent souvent des plug-ins Internet Explorer indésirables, tels que des barres d'outils ou des outils d'aide à la navigation (BHO - Browser Helper Objects).
Modification des paramètres d'Internet Explorer	De nombreux virus/programmes malveillants modifient les paramètres d'Internet Explorer, notamment la page d'accueil, les sites Web de confiance, les paramètres de serveur proxy et les extensions de menu.
Modification des stratégies de sécurité	La modification des stratégies de sécurité de Windows peut permettre à des applications indésirables de s'exécuter puis de changer les paramètres du système.
Injection de bibliothèques de programmes	De nombreux programmes malveillants configurent Windows de telle sorte que toutes les applications chargent automatiquement une bibliothèque de programmes (DLL). Ceci permet aux routines malveillantes contenues dans cette DLL de s'exécuter chaque fois qu'une de ces applications est lancée.
Modification du shell	De nombreux programmes malveillants modifient les paramètres du shell Windows de manière à s'associer eux-mêmes à certains types de fichiers. Cette routine permet à des programmes malveillants de se lancer automatiquement dès qu'un utilisateur ouvre les fichiers associés dans l'Explorateur Windows. La modification des paramètres du shell Windows peut aussi permettre à des programmes malveillants de suivre les programmes utilisés et de s'exécuter conjointement avec les applications légitimes.
Nouveau service	Les services Windows sont des processus dotés de fonctions spéciales qui, généralement, s'exécutent continuellement en arrière-plan et bénéficient d'un accès d'administration complet. Certains programmes malveillants s'installent eux-mêmes en tant que services afin de rester dissimulés.
Modification du système de fichiers	Certains fichiers système de Windows déterminent le comportement du système et notamment les paramètres relatifs aux programmes de démarrage et aux économiseurs d'écran. De nombreux programmes malveillants modifient les fichiers système de manière à s'exécuter automatiquement au démarrage et contrôler le comportement du système.

Événements	Description
Modification des stratégies de pare-feu	La stratégie de pare-feu Windows détermine quelles applications ont accès au réseau, quels ports sont ouverts à la communication et quelles adresses IP peuvent communiquer avec l'ordinateur. De nombreux programmes malveillants modifient la stratégie de manière à s'octroyer à eux-mêmes l'accès au réseau et à Internet.
Modification des processus système	De nombreux programmes malveillants agissent de différentes façons sur les processus Windows intégrés. Ces actions peuvent consister à interrompre ou à modifier les processus en cours d'exécution.
Nouveau programme de démarrage	Les applications malveillantes ont tendance à ajouter ou modifier des entrées de démarrage automatique dans le Registre Windows, afin d'être lancées automatiquement à chaque démarrage de l'ordinateur.

Lorsque la surveillance des événements détecte un événement du système surveillé, elle exécute l'action configurée pour l'événement.

Le tableau suivant répertorie les éventuelles mesures que les administrateurs peuvent prendre sur les événements du système surveillés.

Tableau 8-2. Actions sur les événements du système surveillés

Action	Description
Évaluer	OfficeScan autorise toujours les programmes associés à un événement, mais enregistre cette action dans les journaux pour évaluation. Il s'agit de l'action par défaut pour tous les événements du système surveillés. **Remarque** Cette option n'est pas prise en charge pour l'injection de bibliothèques de programmes sur les systèmes 64 bits.
Autoriser	OfficeScan autorise toujours les programmes associés à un événement.

Action	Description
Demander si nécessaire	OfficeScan invite les utilisateurs à autoriser ou refuser les programmes associés à un événement et ajoute les programmes à la liste d'exceptions Si l'utilisateur ne répond pas au cours d'une certaine période, OfficeScan autorise automatiquement l'exécution du programme. La valeur par défaut de la période est 30 secondes. Pour modifier la période, reportez-vous à *Configuration des paramètres généraux de surveillance des comportements à la page 8-8*. **Remarque** Cette option n'est pas prise en charge pour l'injection de bibliothèques de programmes sur les systèmes 64 bits.
Refuser	OfficeScan bloque toujours les programmes associés à un événement et enregistre cette action dans les journaux. Lorsqu'un programme est bloqué et que les notifications sont activées, OfficeScan affiche une notification sur l'ordinateur OfficeScan. Pour plus de détails sur les notifications, voir *Notifications de surveillance des comportements pour les utilisateurs des agents OfficeScan à la page 8-14*.

Liste d'exceptions de la surveillance des comportements

La liste d'exceptions de la surveillance des comportements contient les programmes n'étant pas surveillés par la surveillance des comportements.

- **Programmes approuvés** : Les programmes de cette liste peuvent être exécutés. Un programme approuvé sera toutefois vérifié par d'autres fonctionnalités de OfficeScan (telles qu'un scan des fichiers) avant que son exécution ne soit définitivement autorisée.
- **Programmes bloqués** : Les programmes de cette liste ne peuvent jamais être démarrés. Pour configurer cette liste, la surveillance des événements doit être activée.

Configurez la liste d'exceptions depuis la console Web. Vous pouvez également donner aux utilisateurs le privilège de configurer leur propre liste des exceptions depuis la

console de l'agent OfficeScan. Pour obtenir des informations détaillées, voir *Privilèges de surveillance des comportements à la page 8-12*.

Configuration du blocage du comportement des programmes malveillants, de la surveillance des événements et de la liste Exception

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Paramètres de surveillance des comportements**.
4. Sélectionnez **Activer le blocage du comportement des programmes malveillants pour les menaces connues et potentielles** et sélectionnez l'une des options suivantes :
    - **Menaces connues** : bloque les comportements associés à des menaces connues liées à des programmes malveillants
    - **Menaces connues et potentielles** : bloque les comportements associés à des menaces connues et entreprend une action sur les comportements potentiellement malveillants
5. Configurez les paramètres de surveillance des comportements.
    a. Sélectionnez **Activer la surveillance des événements**.
    b. Choisissez les événements du système à surveiller et sélectionnez une action pour chacun de ces événements. Pour des informations relatives aux événements du système surveillés et aux actions, voir *Surveillance des événements à la page 8-3*.
6. Configurez la liste des exceptions.
    a. Sous **Saisissez le chemin d'accès complet du programme**, entrez le chemin d'accès complet du programme à approuver ou à bloquer. Séparez les entrées multiples par des points virgules (;).

b. Cliquez sur **Ajouter à la liste des URL approuvées** ou **Ajouter à la liste des URL bloquées**.

c. Pour supprimer de la liste un programme approuvé ou bloqué, cliquez sur l'icône de la corbeille ( ) en regard du programme.



Remarque

OfficeScan accepte au maximum 100 programmes approuvés et 100 programmes bloqués.

7. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :

- **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.
- **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Configuration des paramètres généraux de surveillance des comportements

OfficeScan applique des paramètres de l'agent général à tous les agents ou seulement aux agents disposant de certains privilèges.

Procédure

1. Accédez à **Agents** > **Paramètres de l'agent général**.
2. Accédez à la section **Paramètres de surveillance des comportements**.

3. Configurez les paramètres suivants selon vos besoins :

Option	Description
Autoriser automatiquement le programme si l'utilisateur ne répond pas dans les __ secondes	Ce paramètre fonctionne uniquement si la surveillance des événements est activée et si l'action pour un événement du système surveillé est « Demander si nécessaire ». Cette action demande à l'utilisateur d'autoriser ou de refuser les programmes associés à l'événement. Si l'utilisateur ne répond pas au cours d'une certaine période, OfficeScan autorise automatiquement l'exécution du programme. Pour obtenir des informations détaillées, consultez la section *Surveillance des événements à la page 8-3*.

OPTION	DESCRIPTION
Avertir les utilisateurs avant l'exécution de programmes récemment trouvés ayant été téléchargés via HTTP ou applications de messagerie (plate-formes serveur exclues)	La surveillance des comportements fonctionne en binôme avec les services de réputation de sites Web pour vérifier la prévalence des fichiers téléchargés via des canaux HTTP ou des applications de messagerie. Après la détection d'un fichier « récemment trouvé », les administrateurs peuvent décider d'avertir les utilisateurs avant d'exécuter le fichier. Trend Micro classe un programme comme étant récemment trouvé selon le nombre de détections de fichiers ou l'âge du fichier tels qu'ils sont déterminés par Smart Protection Network. La surveillance des comportements scanne les types de fichiers suivants pour chaque canal : • HTTP : scanne les fichiers `.exe`. • Applications de messagerie électronique : scanne les fichiers `.exe`, ainsi que les fichiers `.exe` compressés dans des fichiers `.zip` et `.rar` non chiffrés. **Remarque** • Les administrateurs doivent activer les services de réputation de sites Web sur l'agent pour autoriser OfficeScan à scanner le trafic HTTP avant de pouvoir afficher cette invite. • Pour les systèmes Windows 7/Vista/XP, cette invite prend uniquement en charge les ports 80, 81 et 8080. • OfficeScan fait correspondre les noms des fichiers téléchargés via des applications de messagerie lors du processus d'exécution. Si le nom de fichier a été modifié, l'utilisateur ne reçoit pas d'invite.

4. Accédez à la section **Paramètres de Certified Safe Software Service** et activez Certified Safe Software Service selon vos besoins.

   Certified Safe Software Service interroge les centres de données Trend Micro pour vérifier la sécurité d'un programme détecté par le blocage du comportement des programmes malveillants, la surveillance des événements, le pare-feu ou les scans

antivirus. Activez le service Certified Safe Software Service pour réduire la probabilité de détection de faux-positifs.



Remarque

Vérifiez que les agents OfficeScan disposent des paramètres proxy corrects (pour plus d'informations, voir *Paramètres proxy des agents OfficeScan à la page 14-51*) avant d'activer Certified Safe Software Service. Des paramètres proxy incorrects, de même qu'une connexion Internet intermittente, peuvent entraîner des retards ou un échec de réception d'une réponse des centres de données Trend Micro, et faire que des programmes apparaissent comme sans réponse.

De plus, les agents OfficeScan IPv6 purs ne peuvent pas interroger directement les centres de données Trend Micro. Un serveur proxy à double pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre aux agents OfficeScan de se connecter aux centres de données Trend Micro.

5. Cliquez sur **Enregistrer**.

Privilèges de surveillance des comportements

Si les agents disposent des privilèges de surveillance des comportements, l'option Surveillance des comportements s'affiche sur l'écran **Paramètres** de la console de l'agent OfficeScan. Les utilisateurs peuvent alors gérer leur propre liste d'exceptions.

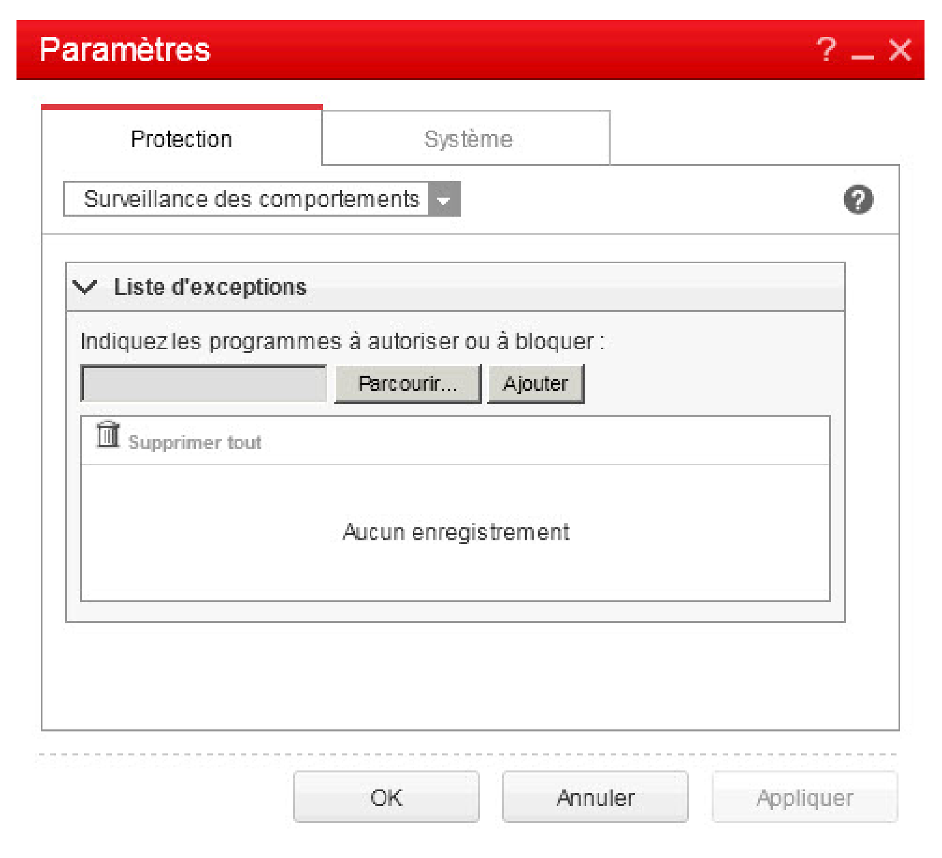


FIGURE 8-1. Option Surveillance des comportements sur la console de l'agent OfficeScan

Autorisation de privilèges de surveillance des comportements

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Dans l'onglet **Privilèges**, allez à la section **Privilèges de surveillance des comportements**.
5. Sélectionnez **Afficher les paramètres de surveillance des comportements sur la console de l'agent OfficeScan**.
6. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :
   - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Notifications de surveillance des comportements pour les utilisateurs des agents OfficeScan

OfficeScan peut afficher un message de notification sur l'ordinateur d'un agent OfficeScan immédiatement après le blocage d'un programme par la surveillance des comportements. Activer l'envoi de messages de notification et modifier éventuellement le contenu du message.

Activation de l'envoi de messages de notification

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Cliquez sur l'onglet **Autres paramètres** et allez à la section **Paramètres de surveillance des comportements**.
5. Sélectionnez **Afficher une notification lorsqu'un programme est bloqué**.
6. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :
   - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet

pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Modification du contenu du message de notification

Procédure

1. Accédez à **Administration** > **Notifications** > **Agent**.
2. Dans la liste déroulante **Type**, sélectionnez **Violations de la stratégie de surveillance des comportements**.
3. Saisissez le message par défaut dans la zone de texte prévue à cet effet.
4. Cliquez sur **Enregistrer**.

Journaux de surveillance des comportements

Les agents OfficeScan consignent dans des journaux les accès non autorisés à des programmes et envoient ces journaux au serveur. Un agent OfficeScan qui s'exécute en permanence regroupe les journaux et les envoie à un intervalle spécifié, qui est de 60 minutes par défaut.

Pour éviter que les journaux n'occupent trop d'espace sur votre disque dur, vous pouvez les supprimer manuellement ou configurer leur suppression programmée. Voir *Gestion du journal à la page 13-36* pour obtenir des informations complémentaires sur la gestion des journaux.

Affichage des journaux de surveillance des comportements

Procédure

1. Accédez à **Journaux** > **Agents** > **Risques de sécurité** ou **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Journaux** > **Journaux de surveillance des comportements** ou **Afficher les journaux** > **Journaux de surveillance des comportements**.
4. Spécifiez les critères de journaux, puis cliquez sur **Afficher les journaux**.
5. Affichez les journaux. Les journaux contiennent les informations suivantes :
    - Date/heure de détection du processus non autorisé
    - Endpoint sur lequel un processus non autorisé a été détecté
    - Domaine du endpoint
    - Violation : règle de surveillance des événements avec laquelle le processus est en infraction
    - Action exécutée lors de la détection de la violation
    - Événement : type d'objet auquel le programme a accédé
    - Niveau de risque que représente le programme non autorisé
    - Programme, c'est-à-dire le programme non autorisé
    - Opération : action exécutée par le programme non autorisé
    - Cible, c'est-à-dire le processus qui a fait l'objet de l'accès

6. Pour sauvegarder les journaux dans un fichier `CSV` (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Configuration de la programmation d'envoi de journaux de surveillance des comportements

---

Procédure

1. Accédez au répertoire <*dossier d'installation du serveur*>`\PCCSRV`.
2. Ouvrez le fichier `ofcscan.ini` à l'aide d'un éditeur de texte comme le Bloc-notes.
3. Recherchez la chaîne « `SendBMLogPeriod` », puis vérifiez la valeur en regard de cette chaîne.

   La valeur par défaut est 3 600 secondes et la chaîne a l'aspect suivant : `SendBMLogPeriod=3600`.
4. Spécifiez la valeur en secondes.

   Par exemple, pour faire passer la période d'envoi des journaux à 2 heures, indiquez 7200 comme valeur.
5. Enregistrez le fichier.
6. Accédez à **Agents** > **Paramètres de l'agent général**.
7. Cliquez sur **Enregistrer** sans changer aucun paramètre.
8. Redémarrez l'agent.



Chapitre 9

Utilisation du contrôle des dispositifs

Ce chapitre explique comment protéger les ordinateurs des risques de sécurité en utilisant la fonctionnalité de contrôle des dispositifs.

Les rubriques sont les suivantes :

Contrôle des dispositifs

Le Contrôle des dispositifs régule l'accès aux périphériques de stockage externes et ressources réseau connectés aux ordinateurs. Le Contrôle des dispositifs prévient la perte et les fuites de données et, conjointement avec le scan de fichiers, contribue à la protection contre les risques de sécurité.

Vous pouvez configurer les stratégies de contrôle des dispositifs pour les agents internes et externes. Les administrateurs OfficeScan configurent généralement une stratégie plus stricte pour les agents externes.

Les stratégies sont des paramètres détaillés dans l'arborescence des agents OfficeScan. Vous pouvez appliquer des stratégies spécifiques à des groupes d'agents ou à des agents individuels. Vous pouvez également appliquer une stratégie unique à tous les agents.

Une fois que vous avez déployé les stratégies, les agents utilisent les critères d'emplacement définis dans l'écran Emplacement de l'ordinateur (voir *Emplacement de l'Endpoint à la page 14-2*) afin de déterminer leur emplacement et la stratégie à appliquer. Les agents changent de stratégie à chaque fois que l'emplacement change.



Important

- Par défaut, le contrôle des dispositifs est désactivé sur toutes les versions de Windows Server 2003, Windows Server 2008 et Windows Server 2012. Avant d'activer le contrôle des dispositifs sur ces plates-formes serveur, consultez les instructions et pratiques recommandées décrites dans *Services de l'agent OfficeScan à la page 14-7*.



Important

- Les types de périphériques pouvant être surveillés par OfficeScan dépendent de l'activation de la licence de protection des données. La protection des données fait l'objet d'une licence distincte et doit être activée avant d'être utilisée. Pour plus d'informations sur la licence de protection des données, voir *Licence de protection des données à la page 3-4*.

TABLEAU 9-1. Types de périphériques

	PROTECTION DES DONNÉES ACTIVÉE	PROTECTION DES DONNÉES DÉSACTIVÉE
Appareils mobiles		
Appareils mobiles	Surveillé	Non surveillé
Périphériques de stockage		
CD/DVD	Surveillé	Surveillé
Disquettes	Surveillé	Surveillé
Lecteurs de réseau	Surveillé	Surveillé
Périphériques de stockage USB	Surveillé	Surveillé
Périphériques qui ne sont pas destinés au stockage		
Cartes Bluetooth	Surveillé	Non surveillé
Ports COM et LPT	Surveillé	Non surveillé
Interface IEEE 1394	Surveillé	Non surveillé
Périphériques d'images	Surveillé	Non surveillé
Périphériques infrarouges	Surveillé	Non surveillé
Modems	Surveillé	Non surveillé
Carte PCMCIA	Surveillé	Non surveillé
Touche Impr. écran	Surveillé	Non surveillé
Cartes d'interface réseau sans fil	Surveillé	Non surveillé

- Pour obtenir la liste des modèles de dispositifs pris en charge, consultez le document *Listes de protection des données* à l'adresse :

  http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Autorisations pour les périphériques de stockage

Les autorisations du contrôle des dispositifs pour les périphériques de stockage sont utilisées dans les cas suivants :

- Lorsque vous autorisez l'accès aux périphériques de stockage USB, CD/DVD, disquettes et lecteurs de réseau. Vous pouvez accorder un accès complet ou limiter le niveau d'accès à ces périphériques.
- Configurez la liste des périphériques de stockage USB approuvés. Le contrôle des dispositifs vous permet de bloquer l'accès à tous les périphériques de stockage USB, sauf ceux qui ont été ajoutés à la liste des périphériques approuvés. Vous pouvez accorder un accès complet aux périphériques approuvés ou limiter le niveau d'accès.

Le tableau suivant répertorie les autorisations d'accès aux périphériques de stockage.

TABLEAU 9-2. Autorisations de contrôle des dispositifs pour les périphériques de stockage

AUTORISATIONS	FICHIERS PRÉSENTS SUR LE PÉRIPHÉRIQUE	FICHIERS ENTRANTS
Accès complet	Opérations autorisées : Copier, Déplacer, Ouvrir, Enregistrer, Supprimer, Exécuter	Opérations autorisées : Enregistrer, Déplacer, Copier En d'autres termes, un fichier peut être enregistré, déplacé et copié sur le périphérique.
Modifier	Opérations autorisées : Copier, Déplacer, Ouvrir, Enregistrer, Supprimer Opérations interdites : Exécuter	Opérations autorisées : Enregistrer, Déplacer, Copier

Autorisations	Fichiers présents sur le périphérique	Fichiers entrants
Lire et exécuter	Opérations autorisées : Copier, Ouvrir, Exécuter Opérations interdites : Enregistrer, Déplacer, Supprimer	Opérations interdites : Enregistrer, Déplacer, Copier
Lire	Opérations autorisées : Copier, Ouvrir Opérations interdites : Enregistrer, Déplacer, Supprimer, Exécuter	Opérations interdites : Enregistrer, Déplacer, Copier
Répertorier le contenu des dispositifs uniquement	Opérations interdites : toutes les opérations Le dispositif et les fichiers qu'il contient sont visibles par l'utilisateur (par exemple, dans l'Explorateur Windows).	Opérations interdites : Enregistrer, Déplacer, Copier
Bloquer (disponible après l'installation de la protection des données)	Opérations interdites : toutes les opérations Le dispositif et les fichiers qu'il contient ne sont pas visibles par l'utilisateur (par exemple, dans l'Explorateur Windows).	Opérations interdites : Enregistrer, Déplacer, Copier

La fonction de scan de fichiers d'OfficeScan complète et, le cas échéant, annule les autorisations relatives aux périphériques. Si, par exemple, l'une d'entre elles autorise l'ouverture d'un fichier mais qu'OfficeScan détecte que celui-ci est infecté par un programme malveillant, une action de scan spécifique est exécutée sur le fichier pour éliminer ce programme. Si l'action de scan est Nettoyer, le fichier s'ouvre une fois le nettoyage effectué. Si, en revanche l'action de scan est Supprimer, le fichier est supprimé.



Conseil

Le contrôle des dispositifs pour la protection des données prend en charge toutes les plates-formes 64 bits. Pour assurer la surveillance de la prévention des modifications non autorisées sur les systèmes non pris en charge par OfficeScan, définissez les autorisations pour les dispositifs sur **Bloquer** pour limiter l'accès à ces périphériques.

Autorisations avancées pour les périphériques de stockage

Les autorisations avancées sont appliquées lorsque vous accordez des autorisations limitées à la plupart des périphériques de stockage. L'autorisation peut être :

- Modifier
- Lire et exécuter
- Lire
- Répertorier le contenu des dispositifs uniquement

Vous pouvez continuer de limiter les autorisations tout en accordant des autorisations avancées à certains programmes sur les périphériques de stockage et sur le endpoint local.

Pour définir des programmes, configurez les listes de programmes suivantes.

TABLEAU 9-3. Listes des programmes

LISTE DES PROGRAMMES	DESCRIPTION	ENTRÉES VALIDES
Programmes disposant d'un accès en lecture et écriture aux périphériques	Cette liste contient des programmes locaux ainsi que des programmes de périphériques de stockage ayant un droit de lecture et d'écriture sur les périphériques. Microsoft Word (`winword.exe`) est un exemple de programme local. Il est généralement situé sous `C:\Program Files\Microsoft Office\Office`. Si l'autorisation d'accès aux périphériques de stockage USB est « Répertorier le contenu des dispositifs uniquement » mais que « `C:\Program Files\Microsoft Office\Office\winword.exe` » est inclus dans cette liste : • un utilisateur aura accès en lecture et écriture à tous les fichiers du périphérique de stockage USB accessibles avec Microsoft Word. • un utilisateur peut enregistrer, déplacer ou copier un fichier Microsoft Word dans le périphérique de stockage USB.	Nom et chemin d'accès du programme Pour obtenir des informations détaillées, voir *Spécification du nom et du chemin d'accès d'un programme à la page 9-9*.
Programmes présents sur les périphériques qui sont autorisés à s'exécuter	Cette liste contient des programmes se trouvant sur les périphériques de stockage et que les utilisateurs ou le système peuvent exécuter. Par exemple, si vous souhaitez autoriser les utilisateurs à installer un logiciel à partir d'un CD, ajoutez le nom et le chemin d'accès du programme d'installation, comme « `E:\Installer\Setup.exe` », à cette liste.	Chemin d'accès et nom du programme ou fournisseur de la signature numérique Pour plus d'informations, voir *Spécification du nom et du chemin d'accès d'un programme à la page 9-9* ou *Spécification d'un fournisseur Digital Signature à la page 9-8*.

Dans certains cas vous devrez ajouter un programme aux deux listes. Prenez par exemple la fonctionnalité de verrouillage de données d'un périphérique de stockage USB qui, si elle est activée, invite l'utilisateur à fournir un nom et un mot de passe avant de déverrouiller le périphérique. La fonctionnalité de verrouillage de données utilise le programme « `Password.exe` » sur le périphérique. Il doit être autorisé à s'exécuter afin que les utilisateurs puissent déverrouiller le périphérique. "`Password.exe` » doit également disposer de droit de lecture et d'écriture sur le périphérique afin que les utilisateurs puissent modifier leur nom d'utilisateur ou leur mot de passe.

Chaque liste de programmes de l'interface utilisateur peut contenir jusqu'à 100 programmes. Si vous souhaitez ajouter plus de programmes à une liste de programmes, vous devrez les ajouter dans le fichier `ofcscan.ini` qui peut accepter un maximum de 1 000 programmes. Pour plus d'informations sur l'ajout de programmes dans le fichier `ofcscan.ini`, voir *Ajout de programmes aux listes de contrôle des dispositifs à l'aide du fichier ofcscan.ini à la page 9-17*.



AVERTISSEMENT!

Les programmes ajoutés au fichier `ofcscan.ini` seront déployés sur le domaine racine et remplaceront les programmes des agents ou domaines individuels.

Spécification d'un fournisseur Digital Signature

Spécifiez un fournisseur de signature digitale si vous faites confiance aux programmes de ce fournisseur. Par exemple, entrez Microsoft Corporation ou Trend Micro, Inc. Vous pouvez obtenir le fournisseur de signature digitale en vérifiant les propriétés d'un

programme (par exemple, en cliquant avec le bouton droit sur le programme et en sélectionnant **Propriétés**).

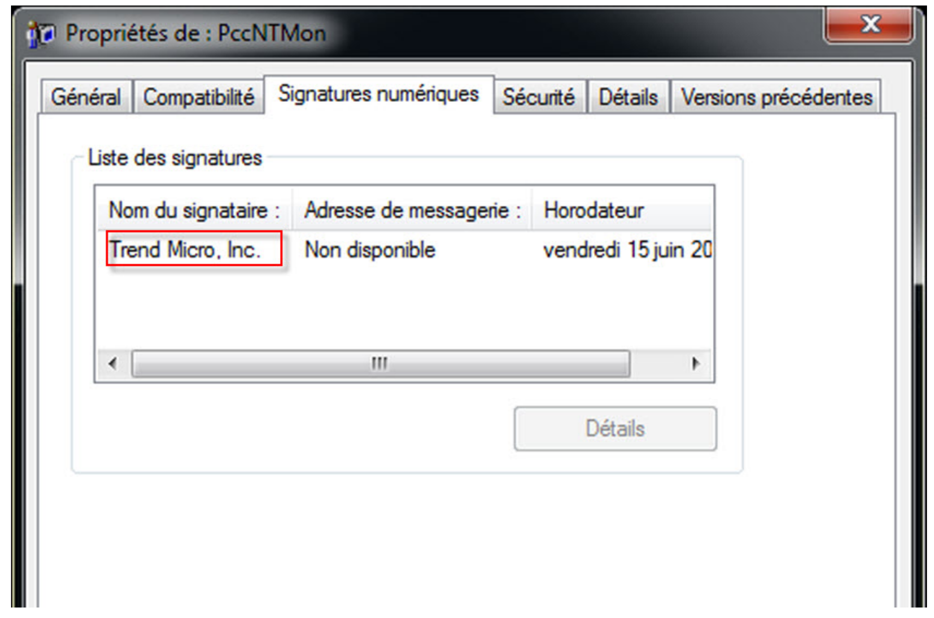


FIGURE 9-1. Fournisseur de signature numérique pour le programme de l'agent OfficeScan (`PccNTMon.exe`)

Spécification du nom et du chemin d'accès d'un programme

Le nome et le chemin d'accès d'un programme doivent compter 259 caractères au maximum et ne peuvent contenir que des caractères alphanumérique (A-Z, a-z, 0-9). Il est impossible de spécifier uniquement le nom du programme.

Vous pouvez utiliser des caractères génériques pour remplacer les lettres de lecteur et les noms de programmes. Utilisez un point d'interrogation (?) pour remplacer un seul caractère, comme la lettre d'un lecteur. Utilisez un astérisque (*) pour remplacer plusieurs caractères, comme un nom de programme.



Remarque

Les caractères génériques ne peuvent pas être utilisés pour remplacer des noms de dossiers. Le nom exact du dossier doit être spécifié.

Les caractères génériques peuvent être utilisés dans les exemples suivants :

TABLEAU 9-4. Utilisation correcte des caractères génériques

EXEMPLE	DONNÉES CORRESPONDANTES
?:\Password.exe	Le fichier «Password.exe» situé dans n'importe quel lecteur
C:\Program Files\Microsoft *.exe	Tout fichier sous C:\Program Files qui possède une extension de fichier
C:\Program Files*.*	Tout fichier sous C:\Program Files qui possède une extension de fichier
C:\Program Files\a**?**c.exe	Tout fichier .exe sous C:\Program Files dont le nom est composé de 3 caractères, commençant par la lettre « a » et se terminant par la lettre « c »
C:*	Tout fichier se trouvant directement sous C:\drive, qu'il possède ou non une extension de fichier

Les caractères génériques ne peuvent pas être utilisés dans les exemples suivants :

TABLEAU 9-5. Utilisation incorrecte des caractères génériques

EXEMPLE	CAUSE
??:\Buffalo\Password.exe	?? représente deux caractères alors qu'une lettre de lecteur n'est composée que d'un seul caractère alphabétique.
*:\Buffalo\Password.exe	* représente plusieurs caractères alors qu'une lettre de lecteur n'est composée que d'un seul caractère alphabétique.
C:*\Password.exe	Les caractères génériques ne peuvent pas être utilisés pour remplacer des noms de dossiers. Le nom exact du dossier doit être spécifié.
C:**?**\Password.exe	

Autorisations pour les périphériques qui ne sont pas destinés au stockage

Vous pouvez autoriser ou bloquer l'accès à des périphériques qui ne sont pas destinés au stockage. Il n'y a pas d'autorisation détaillée ou avancée pour ces périphériques.

Gestion de l'accès aux périphériques externes (protection des données activée)

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Paramètres de contrôle des dispositifs**.
4. Pour configurer des paramètres applicables aux agents externes, cliquez sur l'onglet **Agents externes** ; pour configurer des paramètres applicables aux agents internes, cliquez sur **Agents internes**.
5. Sélectionnez **Activer le contrôle des dispositifs**.
6. Appliquez les paramètres comme suit :
   - Si vous êtes sur l'onglet **Agents externes**, vous pouvez appliquer des paramètres aux agents internes en sélectionnant **Appliquer tous les paramètres aux agents internes**.
   - Si vous êtes sur l'onglet **Agents internes**, vous pouvez appliquer des paramètres aux agents externes en sélectionnant **Appliquer tous les paramètres aux agents externes**.
7. Autorisez ou bloquez la fonction AutoRun (`autorun.inf`) sur les périphériques de stockage USB.
8. Configurez les paramètres pour les périphériques de stockage.

a. Sélectionnez une autorisation pour chaque périphérique de stockage. Pour plus de détails sur les autorisations, voir *Autorisations pour les périphériques de stockage à la page 9-4*.

b. Si l'autorisation pour les périphériques de stockage USB est **Bloquer**, configurez une liste de périphériques approuvés. Les utilisateurs peuvent accéder à ces périphériques et vous pouvez contrôler le niveau d'accès en utilisant les autorisations. Voir la section *Configuration d'une liste approuvée de périphériques USB à la page 9-14*.

9. Pour chaque périphérique non destiné au stockage, sélectionnez **Autoriser** ou **Bloquer**.

10. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :

    - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.

    - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Configuration des autorisations avancées

Bien que vous puissiez configurer des autorisation avancées et des notifications pour un périphérique de stockage spécifique dans l'interface utilisateur, les autorisations et les notifications sont en fait attribuées à tous les périphériques de stockage. Cela signifie que lorsque vous cliquez sur **Autorisations avancées et notifications** pour un CD ou un DVD, vous définissez des autorisations et des notifications pour tous les périphériques de stockage.



Remarque

Pour plus d'informations sur les autorisations avancées et la manière de définir correctement des programmes avec des autorisations avancées, voir *Autorisations avancées pour les périphériques de stockage à la page 9-6*.

Procédure

1. Cliquez sur **Autorisations avancées et notifications**.

   Un nouvel écran s'affiche.

2. Sous **Programmes ayant un droit de lecture et d'écriture sur des périphériques des stockage**, entrez le nom et le chemin d'accès d'un programme, puis cliquez sur **Ajouter**.

   Le fournisseur de la signature digitale n'est pas accepté.

3. Sous **Programmes présents sur les périphériques de stockage et autorisés à s'exécuter**, entrez le nom et le chemin d'accès du programme ou le fournisseur de la signature digitale, puis cliquez sur **Ajouter**.

4. Sélectionnez **Afficher un message de notification sur le endpoint lorsqu'OfficeScan détecte un accès non autorisé à un périphérique**.

   - Un accès non autorisé à un périphérique fait référence à des opérations interdites. Par exemple, si l'autorisation pour le périphérique est «Lire», les utilisateurs ne pourront pas enregistrer, déplacer, supprimer ou exécuter un fichier sur le périphérique. Pour une liste d'opérations interdites sur le périphériques sur base des autorisations, voir *Autorisations pour les périphériques de stockage à la page 9-4*.

   - Vous pouvez modifier le message de notification. Pour obtenir des informations détaillées, voir *Modification des notifications du contrôle des dispositifs à la page 9-18*.

5. Cliquez sur **Retour**.

Configuration d'une liste approuvée de périphériques USB

La liste approuvée pour les périphériques USB prend en charge l'utilisation de l'astérisque (*) comme caractère générique. Remplacez tout champ avec l'astérisque (*) pour inclure tous les périphériques répondant aux autres champs. Par exemple, [vendeur]-[modèle]-* place tous les dispositifs USB du vendeur et du type de modèle spécifiés dans la liste approuvée, peu importe l'ID de série.

Procédure

1. Cliquez sur **Périphériques approuvés**
2. Saisissez le vendeur du périphérique
3. Saisissez le modèle et l'ID de série du périphérique.



Conseil

À l'aide de l'outil Liste de dispositifs, interrogez les dispositifs reliés aux endpoints. L'outil indique, pour chaque périphérique, le nom du fournisseur, le modèle et le numéro de série. Pour obtenir des informations détaillées, consultez la section *Outil Liste de dispositifs à la page 9-14*.

---

4. Sélectionnez la permission pour le périphérique.

   Pour plus de détails sur les autorisations, voir *Autorisations pour les périphériques de stockage à la page 9-4*.

5. Pour ajouter plusieurs périphériques, cliquez sur l'icône plus (**+**).
6. Cliquez sur **< Retour**.

Outil Liste de dispositifs

Exécutez localement l'outil Liste de dispositifs sur chaque endpoint pour interroger les dispositifs externes qui y sont connectés. L'outil scanne un endpoint à la recherche de dispositifs externes, puis affiche les informations relatives à ce dispositif dans une fenêtre de navigateur. Vous pouvez ensuite utiliser les informations lors de la

configuration des paramètres des dispositifs pour la prévention contre la perte de données et le contrôle des dispositifs.

Exécution de l'outil Liste de dispositifs

Procédure

1. Sur l'ordinateur du serveur OfficeScan, accédez au répertoire `\PCCSRV\Admin\Utility\ListDeviceInfo`.
2. Copiez `listDeviceInfo.exe` sur le endpoint cible.
3. Sur le endpoint, double-cliquez sur `listDeviceInfo.exe`.
4. Les informations relatives au dispositif s'affichent dans la fenêtre de navigation qui s'ouvre. La prévention contre la perte de données et le contrôle des dispositifs utilisent les informations suivantes :
   - Revendeur (obligatoire)
   - Modèle (facultatif)
   - ID de série (facultatif)

Gestion de l'accès aux périphériques externes (protection des données non activée)

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Paramètres de contrôle des dispositifs**.
4. Pour configurer des paramètres applicables aux agents externes, cliquez sur l'onglet **Agents externes** ; pour configurer des paramètres applicables aux agents internes, cliquez sur **Agents internes**.

5. Sélectionnez **Activer le contrôle des dispositifs**.

6. Appliquez les paramètres comme suit :

    - Si vous êtes sur l'onglet **Agents externes**, vous pouvez appliquer des paramètres aux agents internes en sélectionnant **Appliquer tous les paramètres aux agents internes**.

    - Si vous êtes sur l'onglet **Agents internes**, vous pouvez appliquer des paramètres aux agents externes en sélectionnant **Appliquer tous les paramètres aux agents externes**.

7. Autorisez ou bloquez la fonction AutoRun (`autorun.inf`) sur les périphériques de stockage USB.

8. Sélectionnez une autorisation pour chaque périphérique de stockage. Pour plus de détails sur les autorisations, voir *Autorisations pour les périphériques de stockage à la page 9-4*.

9. Configurez des autorisations avancées et des notifications si l'autorisation pour un périphérique de stockage est l'une des suivantes : **Modifier**, **Lire et exécuter**, **Lire** ou **Répertorier le contenu des dispositifs uniquement**. Voir la section *Configuration des autorisations avancées à la page 9-12*.

10. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :

    - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.

    - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Ajout de programmes aux listes de contrôle des dispositifs à l'aide du fichier ofcscan.ini



Remarque

Pour plus d'informations sur les listes de programmes et la manière de définir correctement les programmes pouvant être ajoutés à la liste, voir *Autorisations avancées pour les périphériques de stockage à la page 9-6*.

Procédure

1. Sur l'ordinateur du serveur OfficeScan, accédez au répertoire <*dossier d'installation du serveur*>`\PCCSRV`.
2. Ouvrez le fichier `ofcscan.ini` à l'aide d'un éditeur de texte.
3. Pour ajouter des programmes disposant d'un accès en lecture et écriture sur les périphériques de stockage :
    a. Localisez les lignes suivantes :

    ```
    [DAC_APPROVED_LIST]
    Count=x
    ```

    b. Remplacez «x» par le nombre de programmes de la liste de programmes.

    c. Sous «Count=x», ajoutez des programmes en entrant :

    ```
    Item<numéro>=<chemin d'accès et nom du programme ou fournisseur de la signature numérique>
    ```

    Par exemple :

    ```
    [DAC_APPROVED_LIST]
    Count=3
    Item0=C:\Program Files\program.exe
    Item1=?:\password.exe
    Élément 2 = Microsoft Corporation
    ```

4. Pour ajouter des programmes présents sur les périphériques de stockage et autorisés à s'exécuter :

   a. Localisez les lignes suivantes :

   ```
   [DAC_EXECUTABLE_LIST]

   Count=x
   ```

   b. Remplacez «x» par le nombre de programmes de la liste de programmes.

   c. Sous «Count=x», ajoutez des programmes en entrant :

   ```
   Item<numéro>=<chemin d'accès et nom du programme ou
   fournisseur de la signature numérique>
   ```

   Par exemple :

   ```
   [DAC_EXECUTABLE_LIST]

   Count=3

   Item0=?:\Installer\Setup.exe

   Item1=E:\*.exe

   Item2=Trend Micro, Inc.
   ```

5. Enregistrez et fermez le fichier `ofcscan.ini`.

6. Ouvrez la console Web OfficeScan et accédez à **Agents** > **Paramètres de l'agent général**.

7. Cliquez sur **Enregistrer** pour déployer les listes de programmes sur tous les agents.

Modification des notifications du contrôle des dispositifs

En cas de violation du contrôle des dispositifs, des messages de notification s'affichent sur les endpoints. Si nécessaire, les administrateurs peuvent également modifier le message de notification par défaut.

Procédure

1. Accédez à **Administration** > **Notifications** > **Agent**.
2. Dans la liste déroulante **Type**, sélectionnez **Violations du contrôle des dispositifs**.
3. Saisissez les messages par défaut dans la zone de texte prévue à cet effet.
4. Cliquez sur **Enregistrer**.

Journaux de contrôle des dispositifs

Les agents OfficeScan consignent dans des journaux les accès non autorisés à des périphériques et envoient ces journaux au serveur. Tout agent qui s'exécute en permanence regroupe les journaux et les envoie toutes les 1 heures. Dès qu'un agent est redémarré, son système vérifie à quel moment les journaux ont été envoyés au serveur pour la dernière fois. Si le délai écoulé dépasse 1 heure, cet agent envoie les journaux immédiatement.

Pour éviter que les journaux n'occupent trop d'espace sur votre disque dur, vous pouvez les supprimer manuellement ou configurer leur suppression programmée. Voir *Gestion du journal à la page 13-36* pour obtenir des informations complémentaires sur la gestion des journaux.

Affichage des journaux de contrôle des dispositifs



Remarque

Seules les tentatives d'accès à des **Périphériques de stockage** sont consignées dans les journaux. Les agents OfficeScan bloquent ou autorisent l'accès à des **Périphériques qui ne sont pas destinés au stockage**, selon la configuration, mais ne consignent pas cette action.

Procédure

1. Accédez à **Journaux** > **Agents** > **Risques de sécurité** ou **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Journaux** > **Journaux de contrôle des dispositifs** ou **Afficher les journaux** > **Journaux de contrôle des dispositifs**.
4. Spécifiez les critères de journaux, puis cliquez sur **Afficher les journaux**.
5. Affichez les journaux. Les journaux contiennent les informations suivantes :
    - Détection d'un accès non autorisé Date/Heure
    - Endpoint auquel est connecté un périphérique externe ou sur lequel est mappée une ressource réseau
    - Domaine du endpoint auquel est connecté un périphérique externe ou sur lequel est mappée une ressource réseau
    - Type de périphérique ou ressource réseau accédés
    - Cible, qui est l'élément accédé sur le périphérique ou la ressource réseau
    - Accédé par, qui spécifie le lieu d'où l'accès a été lancé
    - Autorisations accordées pour la cible
6. Pour sauvegarder les journaux dans un fichier `CSV` (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.



Chapitre 10

Utilisation de la prévention contre la perte de données

Ce chapitre explique comment utiliser la fonctionnalité de prévention contre la perte de données.

Les rubriques sont les suivantes :

À propos de la prévention contre la perte de données

Les solutions de sécurité classiques sont destinées à empêcher les menaces de sécurité externes d'atteindre le réseau. Dans l'environnement de sécurité actuel, elles s'avèrent incomplètes. Les failles de sécurité sont désormais monnaie courante et exposent les données sensibles et confidentielles d'une organisation (appelées des actifs numériques) à des entités externes non autorisées. Une faille de sécurité peut résulter d'erreurs ou de négligences des employés internes, de l'externalisation des données, d'ordinateurs volés ou égarés, ou d'attaques malveillantes.

Les violations de données peuvent :

- Porter préjudice à la réputation de la marque
- Diminuer la confiance des clients envers l'organisation
- Entraîner des coûts supplémentaires pour couvrir la réparation et le paiement d'amandes pour violation des règles de conformité
- Mener à la perte d'opportunités commerciales et de chiffre d'affaires lorsque la propriété intellectuelle est volée

Du fait de la fréquence et des effets dramatiques des violations de données, les organisations considèrent dorénavant la protection des actifs numériques comme un composant décisif de leur infrastructure de sécurité.

La prévention contre la perte de données protège les données sensibles de l'entreprise contre toute fuite accidentelle ou délibérée. La prévention contre la perte des données permet ce qui suit :

- Identifiez les informations sensibles exigeant une protection à l'aide d'identificateurs de données
- La création de stratégies qui limitent ou empêchent la transmission d'actifs numériques par les canaux de transmission classiques, tels que les e-mails et les dispositifs externes.
- Le renforcement de la conformité à des normes de confidentialité établies

Avant de pouvoir contrôler une perte potentielle des informations sensibles, vous devez être en mesure de répondre aux questions suivantes :

- Quelles données doivent être protégées des utilisateurs non autorisés ?
- Où se trouvent les données sensibles ?
- Comment sont transmises les données sensibles ?
- Quels sont les utilisateurs autorisés à accéder ou transmettre les données sensibles ?
- Quelle action doit être entreprise en cas de violation de la sécurité ?

Cet audit primordial implique en général plusieurs départements et membres du personnel au courant des informations sensibles de votre entreprise.

Si vous avez déjà défini les informations sensibles et les stratégies de sécurité, vous pouvez commencer à définir les identificateurs de données ainsi que les stratégies d'entreprise.

Stratégies de prévention contre la perte de données

OfficeScan évalue un fichier ou des données par rapport à un ensemble de règles définies dans les stratégies de prévention contre la perte de données. Les stratégies déterminent les fichiers ou les données qui doivent être protégés des transmissions non autorisées et l'action qu'OfficeScan doit effectuer lorsqu'il détecte une transmission.



Remarque

OfficeScan ne contrôle pas les transmissions de données entre le serveur et les agents OfficeScan.

OfficeScan vous donne la possibilité de configurer des stratégies pour les agents OfficeScan internes et externes. Les administrateurs configurent généralement une stratégie plus stricte pour les agents externes.

Les administrateurs peuvent appliquer des stratégies spécifiques à des groupes d'agents ou à des agents individuels.

Une fois que vous avez déployé les stratégies, les agents utilisent les critères d'emplacement définis dans l'écran **Emplacement de l'Endpoint** (voir *Emplacement de l'Endpoint à la page 14-2*le *Manuel de l'administrateur OfficeScan*)) afin de déterminer leur emplacement et la stratégie à appliquer. Les agents changent de stratégie à chaque fois que l'emplacement change.

Configuration de la stratégie

Définissez les stratégies DLP en configurant les paramètres suivants et en les déployant sur les agents sélectionnés :

Tableau 10-1. Paramètres définissant une stratégie de prévention contre de la perte de données

Paramètres	Description
Règles	Une règle de prévention contre la perte de données peut consister en plusieurs modèles, canaux et actions. Chaque règle est un sous-ensemble de la stratégie de prévention contre la perte de données globale. **Remarque** La prévention contre la perte de données traite les règles et les modèles selon leur ordre de priorité. Si une règle est définie sur « Ignorer », la prévention contre la perte de données traite la règle suivante de la liste. Si une règle est définie sur « Bloquer » ou « Justification de l'utilisateur », la prévention contre la perte de données bloque ou accepte l'action de l'utilisateur et interrompt le traitement de cette règle ou de ce modèle.

PARAMÈTRES	DESCRIPTION
Modèles	Un modèle de prévention contre la perte de données réunit les identificateurs de données et les opérateurs logiques (Et, Ou, Sauf) pour former des conditions. Seuls les fichiers ou les données qui satisfont à certaines conditions feront l'objet d'une règle DLP. La prévention contre la perte de données est fournie avec un ensemble de modèles prédéfinis et permet aux administrateurs de créer des modèles personnalisés. Une règle de prévention contre la perte de données peut contenir un ou plusieurs modèles. La prévention contre la perte de données utilise la règle de première correspondance lors de la vérification des modèles. Cela signifie que si un fichier ou des données correspondent aux identificateurs de données d'un modèle, la prévention contre la perte de données ne vérifiera plus les autres modèles.
Canaux	Les canaux sont des entités de transmission d'informations sensibles. La prévention contre la perte de données prend en charge les canaux de transmission les plus populaires, tels que les courriers électroniques, les périphériques de stockage amovibles et les applications de messagerie instantanée.
Actions	La prévention contre la perte de données exécute une ou plusieurs actions lorsqu'elle détecte une tentative de transmission d'informations sensibles via n'importe quel canal.
Exceptions	Les exceptions remplacent les règles de prévention contre la perte de données. Configurez les exceptions pour gérer le scan des cibles non contrôlées, des cibles contrôlées et des fichiers compressés.
Identificateurs de données	La prévention contre la perte de données utilise des identificateurs de données pour identifier les informations sensibles. Les identificateurs de données comprennent des expressions, attributs de fichier et mots-clés qui agissent en tant qu'unités de constitution des modèles de prévention contre la perte de données.

Types d'identificateurs de données

Les actifs numériques sont des fichiers et des données qu'une entreprise doit protéger contre les transmissions non autorisées. Vous pouvez définir les actifs numériques à l'aide des identificateurs de données suivants :

- **Expressions** : Données ayant une certaine structure. Pour obtenir des informations détaillées, voir *Expressions à la page 10-6*.
- **Attributs de fichier** : Propriétés d'un fichier, telles que son type ou sa taille. Pour obtenir des informations détaillées, voir *Attributs de fichier à la page 10-12*.
- **Liste des mots-clés** : Liste de mots ou d'expressions particuliers. Pour obtenir des informations détaillées, voir *Mots-clés à la page 10-14*.



Remarque

Il n'est pas possible de supprimer un identificateur de données qui est utilisé dans un modèle DLP. Supprimez le modèle pour pouvoir supprimer l'identificateur de données.

Expressions

Une expression est constituée de données ayant une certaine structure. Par exemple, une carte de crédit possède généralement un numéro à 16 chiffres, présenté sous le format « nnnn-nnnn-nnnn-nnnn », pouvant être localisé lors d'une détection basée sur les expressions.

Vous pouvez utiliser des expressions prédéfinies et personnalisées. Pour obtenir des informations détaillées, voir *Expressions prédéfinies à la page 10-6* et *Expressions personnalisées à la page 10-7*.

Expressions prédéfinies

La prévention contre la perte de données est fournie avec un ensemble d'expressions prédéfinies. Ces expressions ne peuvent pas être modifiées ou supprimées.

La prévention contre la perte de données vérifie ces expressions au moyen du processus de vérification de la correspondance des fichiers de signatures et d'équations

mathématiques. Lorsque la prévention contre la perte de données fait correspondre des données potentiellement sensibles avec une expression, les données peuvent également être soumises à des vérifications supplémentaires.

Pour obtenir la liste complète des expressions prédéfinies, consultez le document *Listes de protection des données* à l'adresse http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Affichage des paramètres des expressions prédéfinies



Remarque

Les expressions prédéfinies ne peuvent pas être modifiées ou supprimées.

Procédure

1. Accédez à **Prévention contre la perte de données** > **Identificateurs de données**.
2. Cliquez sur l'onglet **expression**.
3. Cliquez sur le nom de l'expression.
4. Consultez les paramètres sur l'écran qui s'affiche.

Expressions personnalisées

Si aucune des expressions prédéfinies ne correspond à vos besoins, vous avez la possibilité d'en créer des personnalisées.

Les expressions constituent un outil puissant de correspondance de chaînes. Avant de procéder à la création d'expressions, vérifiez que vous maîtrisez la syntaxe des expressions. Les expressions mal formulées peuvent avoir un impact conséquent sur les performances.

Lorsque vous créez des expressions :

- Reportez-vous aux expressions prédéfinies pour savoir comment définir une expression valide. Par exemple, si vous créez une expression qui comprend une date, vous pouvez vous référer aux expressions précédées de «Date».
- Remarque : la prévention contre la perte de données respecte les formats d'expression définis dans la bibliothèque Perl Compatible Regular Expressions (PCRE). Pour plus d'informations sur PCRE, visitez le site Web suivant :

  http://www.pcre.org/
- Commencez par des expressions simples. Modifiez les expressions si celles-ci déclenchent de fausses alertes, ou ajustez-les pour améliorer les détections.

Lors de la création d'expressions, plusieurs critères sont à votre disposition. Une expression doit correspondre aux critères que vous avez choisis pour que la prévention contre la perte de données puisse la soumettre à une stratégie DLP. Pour plus de détails sur les différentes actions, reportez-vous à *Critères applicables aux expressions personnalisées à la page 10-8*.

Critères applicables aux expressions personnalisées

TABLEAU 10-2. Options de critères pour des expressions personnalisées

CRITÈRES	RÈGLE	EXEMPLE
Aucune	Aucune	Tous - Noms du Bureau du recensement des États-Unis • Expression : [^\w]([A-Z][a-z]{1,12}(\s?,\s?|[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]
Caractères spécifiques	Une expression doit intégrer les caractères que vous avez spécifiés. De plus, le nombre de caractères de l'expression doit être compris dans les limites minimale et maximale définies.	États-Unis - Numéro de routage ABA • Expression : [^\d]([0123678]\d{8})[^\d] • Caractères : 0123456789 • Nombre de caractères minimal : 9 • Nombre de caractères maximal : 9

Critères	Règle	Exemple
Suffixe	Le suffixe correspond au dernier segment d'une expression. Un suffixe doit compter un certain nombre de caractères et inclure ceux que vous avez spécifiés. De plus, le nombre de caractères de l'expression doit être compris dans les limites minimale et maximale définies.	Tous - Adresse de domicile • Expression : \D(\d+\s[a-z.]+\s([a-z]+\s){0,2} (lane|ln|street|st|avenue|ave| road|rd|place|pl|drive|dr|circle| cr|court|ct|boulevard|blvd)\.? [0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\s\d{5}(-\d{4})?)[^\d-] • Caractères pour le suffixe : 0123456789- • Nombre de caractères : 5 • Nombre de caractères minimal dans l'expression : 25 • Nombre de caractères maximal dans l'expression : 80
Un seul caractère de séparation	Une expression doit comporter deux segments séparés par un caractère. Le caractère doit avoir une longueur d'un octet. De plus, le nombre de caractères situés à gauche du séparateur doit être compris dans les limites minimale et maximale définies. Le nombre de caractères situés à droite ne doit pas dépasser la limite maximale.	Tous - Adresse électronique • Expression : [^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] • Séparateur : @ • Nombre de caractères minimal à gauche : 3 • Nombre de caractères maximal à gauche : 15 • Nombre de caractères maximal à droite : 30

Création d'une expression personnalisée

Procédure

1. Accédez à **Prévention contre la perte de données** > **Identificateurs de données**.

2. Cliquez sur l'onglet **expression**.

3. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.

4. Entrez un nom pour l'expression. La longueur du nom ne doit pas être supérieure à 100 octets. Le nom ne peut pas contenir les caractères suivants :

   - > < * ^ | & ? \ /

5. Saisissez une description ne dépassant pas 256 octets.

6. Saisissez l'expression et indiquez si celle-ci respecte la casse.

7. Saisissez les données affichées.

   Par exemple, si vous créez une expression pour des numéros ID, saisissez un exemple de numéro ID. Ces données sont utilisées à des fins de référence uniquement et ne figureront pas sur le produit.

8. Choisissez l'un des critères suivants, puis configurez des paramètres complémentaires pour ce critère (voir *Critères applicables aux expressions personnalisées à la page 10-8*) :

   - Aucune
   - Caractères spécifiques
   - Suffixe
   - Un seul caractère de séparation

9. Testez l'expression avec des données réelles.

   Par exemple, si l'expression s'applique à un ID national, entrez un numéro ID valide dans la zone de texte **Données de test**, cliquez sur **Tester**, puis vérifiez le résultat.

10. Cliquez sur **Enregistrer** si vous êtes satisfait du résultat.



Remarque

Enregistrez les paramètres uniquement si le test a réussi. Une expression qui ne détecte aucune donnée consomme les ressources du système inutilement et peut avoir une influence négative sur les performances.

11. Un message s'affiche, vous rappelant de déployer les paramètres vers les agents. Cliquez sur **Fermer**.

12. Lorsque vous êtes à nouveau sur l'écran **Identificateurs de données DLP**, cliquez sur **Appliquer à tous les agents**.

Importation d'une expression personnalisée

Si le formatage du fichier `.dat` contenant les expressions est approprié, utilisez cette fonction. Pour générer le fichier, vous pouvez exporter les expressions à partir du serveur actif ou à partir de tout autre serveur.



Remarque

Les fichiers d'expression `.dat` générés par cette version de la prévention contre la perte de données ne sont pas compatibles avec les versions précédentes.

Procédure

1. Accédez à **Prévention contre la perte de données** > **Identificateurs de données**.

2. Cliquez sur l'onglet **expression**.

3. Cliquez sur **Importer**, puis localisez le fichier `.dat` contenant les expressions.

4. Cliquez sur **Ouvrir**.

   Un message s'affiche et vous informe de la réussite ou de l'échec de l'importation. Si une expression à importer existe déjà, elle sera ignorée.

5. Cliquez sur **Appliquer à tous les agents**.

Attributs de fichier

Les attributs de fichier sont des propriétés spécifiques à un fichier. Vous pouvez utiliser deux attributs de fichier lorsque vous définissez des identificateurs de données, à savoir le type de fichier et la taille de fichier. Par exemple, une entreprise de développement de logiciels souhaitera peut-être limiter le partage du programme d'installation du logiciel de l'entreprise aux membres du service de recherche et développement, lesquels sont chargés de développer et tester le logiciel. Dans ce cas, l'administrateur OfficeScan peut créer une stratégie qui bloque la transmission des fichiers exécutables de 10 à 40 Mo vers l'ensemble des départements, à l'exception de celui de recherche et de développement.

Les attributs de fichier ne permettent pas, en tant que tels, d'identifier les fichiers sensibles. Si nous reprenons l'exemple cité dans cette rubrique, les programmes d'installation de logiciels tiers partagés par d'autres départements risquent d'être bloqués. Par conséquent, Trend Micro recommande d'associer les attributs de fichier à d'autres identificateurs de données pour la prévention contre la perte de données, ce, pour permettre une détection plus ciblée des fichiers sensibles.

Pour obtenir la liste complète des types de fichiers pris en charge, consultez le document *Listes de protection des données* à l'adresse http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Création d'une liste d'attributs de fichier

Procédure

1. Accédez à **Prévention contre la perte de données** > **Identificateurs de données**.

2. Cliquez sur l'onglet **attribut de fichier**.

3. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.

4. Saisissez un nom pour la liste d'attributs de fichier. La longueur du nom ne doit pas être supérieure à 100 octets. Le nom ne peut pas contenir les caractères suivants :

   - > < * ^ | & ? \ /

5. Saisissez une description ne dépassant pas 256 octets.

6. Sélectionnez vos véritables types de fichiers favoris.

7. Si un type de fichier que vous souhaitez inclure n'est pas répertorié, sélectionnez **Extensions de fichier** et entrez l'extension du type de fichier. La prévention contre la perte de données vérifie les fichiers contenant l'extension spécifiée mais pas le véritable type de fichier. Directives à suivre lorsque vous saisissez des extensions de fichiers :

   - Chaque extension doit commencer par un astérisque (*), suivi d'un point (.) et ensuite de l'extension. L'astérisque est un caractère générique qui représente un nom réel de fichier. Par exemple, `*.pol` correspond à `12345.pol` et `test.pol`.

   - Vous pouvez inclure des caractères génériques dans les extensions. Utilisez un point d'interrogation (?) pour représenter un seul caractère et un astérisque (*) pour deux caractères ou plus. Voir les exemples suivants :

     - `*.*m` correspond aux fichiers suivants : `ABC.dem`, `ABC.prm`, `ABC.sdcm`

     - `*.m*r` correspond aux fichiers suivants : `ABC.mgdr`, `ABC.mtp2r`, `ABC.mdmr`

     - `*.fm?` correspond aux fichiers suivants : `ABC.fme`, `ABC.fml`, `ABC.fmp`

   - Faites attention si vous utilisez un astérisque à la fin d'une extension car il peut correspondre à des parties de noms de fichiers et à une extension sans rapport. Par exemple : `*.do*` correspond à `abc.doctor_john.jpg` et `abc.donor12.pdf`.

   - Utilisez les points-virgules (;) pour séparer les extensions de fichier. Il n'est pas nécessaire d'ajouter un espace après un point-virgule.

8. Entrez les tailles de fichier minimale et maximale en octets. Les valeurs doivent être des entiers non nuls.

9. Cliquez sur **Enregistrer**.

10. Un message s'affiche, vous rappelant de déployer les paramètres vers les agents. Cliquez sur **Fermer**.

11. Lorsque vous êtes à nouveau sur l'écran **Identificateurs de données DLP**, cliquez sur **Appliquer à tous les agents**.

Importation d'une liste d'attributs de fichier

Si le formatage du fichier `.dat` contenant les listes d'attributs de fichier est approprié, utilisez cette fonction. Pour générer le fichier, vous pouvez exporter les listes d'attributs de fichier à partir du serveur actif ou à partir de tout autre serveur.



Remarque

Les fichiers d'attributs `.dat` générés par cette version de la prévention contre la perte de données ne sont pas compatibles avec les versions précédentes.

Procédure

1. Accédez à **Prévention contre la perte de données** > **Identificateurs de données**.

2. Cliquez sur l'onglet **attribut de fichier**.

3. Cliquez sur **Importer**, puis localisez le fichier `.dat` contenant les listes d'attributs de fichier.

4. Cliquez sur **Ouvrir**.

   Un message s'affiche et vous informe de la réussite ou de l'échec de l'importation. Si une liste d'attributs de fichier à importer existe déjà, elle sera ignorée.

5. Cliquez sur **Appliquer à tous les agents**.

Mots-clés

Les mots-clés sont des expressions ou des mots spéciaux. Vous pouvez ajouter des mots-clés de la même famille à une liste de mots-clés afin d'identifier un certain nombre de données spécifiques. Par exemple, «pronostic», «groupe sanguin», «vaccination» et «médecin» sont des mots-clés pouvant apparaître dans un certificat médical. Si vous

souhaitez éviter la transmission de fichiers contenant des certificats médicaux, vous pouvez utiliser ces mots-clés dans une stratégie DLP, puis configurer la prévention contre la perte de données pour qu'elle bloque les fichiers contenant ces mots-clés.

Les mots habituellement utilisés peuvent être associés afin de former des mots-clés significatifs. Par exemple, «end», «read», «if» et «at» peuvent être associés pour former des mots-clés présents dans du code source, tels que «END-IF», «END-READ» et «AT END».

Vous pouvez utiliser des listes de mots-clés prédéfinies et personnalisées. Pour obtenir des informations détaillées, voir *Listes de mots-clés prédéfinies à la page 10-15* et *Listes de mots-clés personnalisées à la page 10-16*.

Listes de mots-clés prédéfinies

La prévention contre la perte de données est fournie avec un ensemble de listes de mots-clés prédéfinies. Ces listes de mots-clés ne peuvent pas être modifiées ou supprimées. Chaque liste a ses propres conditions intégrées qui déterminent si le modèle doit déclencher une violation de stratégie.

Pour plus d'informations sur les listes de mots-clés prédéfinies dans la prévention contre la perte de données, consultez le document *Listes de protection des données* à l'adresse http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Fonctionnement des listes de mots-clés

Condition de nombre de mots-clés

Chaque liste de mots-clés contient une condition qui requiert qu'un certain nombre de mots-clés existe dans un document avant que la liste ne déclenche une violation.

La condition du nombre de mots-clés contient les valeurs suivantes :

- **Tous** : Tous les mots-clés de la liste doivent exister dans le document.
- **Tout** : N'importe quel mot-clé de la liste doit exister dans le document.

- **Nombre spécifique** : Le document doit comporter au moins le nombre spécifié de mots-clés. S'il y a plus de mots-clés dans le document que le nombre spécifié, la prévention contre la perte de données déclenche une violation.

Condition de distance

Certaines des listes contiennent une condition de « distance » pour savoir si une violation est présente. « Distance » se réfère au nombre de caractères existant entre le premier caractère d'un mot clé et le premier caractère d'un autre mot-clé. L'entrée suivante peut servir d'exemple :

Prénom :_John_ Nom :_Smith_

La liste des **Formulaires - Prénom, nom** comporte une condition de « distance » de cinquante (50) et les champs de formulaire couramment utilisés de « Prénom » et « Nom ». Dans l'exemple ci-dessus, la prévention contre la perte de données déclenche une violation car le nombre de caractères entre le « P » de « prénom » et le « N » de « nom » est égal à dix-huit (18).

Voici un exemple d'entrée qui ne déclenche pas de violation :

Le P**rénom de notre nouvel employé de Suisse est John. Son N**om est Smith.

Dans cet exemple, le nombre de caractères entre le « p » de « prénom » et le « n » de « nom » est soixante et un (61). Cela dépasse le seuil de distance et ne déclenche pas de violation.

Listes de mots-clés personnalisées

Si aucune des listes de mots-clés prédéfinies ne correspond à vos besoins, vous avez la possibilité d'en créer des personnalisées.

Lors de la configuration d'une liste de mots-clés, plusieurs critères sont à votre disposition. Une liste de mots-clés doit correspondre aux critères que vous avez choisis avant que la prévention contre la perte de données ne puisse la soumettre à une stratégie. Pour chaque liste de mots-clés, choisissez l'un des critères suivants :

- **N'importe quel mot-clé**
- **Tous les mots-clés**

- **Tous les mots-clés de <x> caractères maximum**
- **Le score combiné des mots-clés dépasse le seuil**

Pour plus d'informations concernant les règles de critères, voir *Critères des listes personnalisées de mots-clés à la page 10-17*.

Critères des listes personnalisées de mots-clés

TABLEAU 10-3. Critères pour une liste de mots-clés

CRITÈRES	RÈGLE
N'importe quel mot-clé	Un fichier doit contenir au moins un mot-clé de la liste.
Tous les mots-clés	Le fichier doit contenir tous les mots-clés de la liste.
Tous les mots-clés de <x> caractères maximum	Le fichier doit contenir tous les mots-clés de la liste. En outre, toute paire de mots-clés doit différer au plus de <x> caractères l'une par rapport à l'autre. Par exemple, vos 3 mots-clés sont WEB, DISK et USB, et le nombre de caractères que vous avez indiqué est 20. Si la prévention contre la perte de données détecte tous les mots-clés dans l'ordre DISK, WEB et USB, le nombre de caractères du « D » (de DISK) au « W » (de WEB) et de ce « W » au « U » (de USB) doit être inférieur ou égal à 20 caractères. Les données suivantes correspondent au critère : DISK####WEB############USB Les données suivantes ne correspondent pas au critère : DISK*******************WEB****USB(23 caractères entre le « D » et le « W ») Lorsque vous déterminez le nombre de caractères, gardez à l'esprit qu'un petit nombre, tel que 10, permettra généralement un scan plus rapide, mais couvrira uniquement une zone relativement restreinte. La plage de détection des données sensibles risque donc d'être limitée, en particulier pour les fichiers volumineux. Plus le nombre est grand, plus la zone couverte est importante et plus la durée du scan est longue.

CRITÈRES	RÈGLE
Le score combiné des mots-clés dépasse le seuil	Un fichier doit contenir un ou plusieurs mots-clés de la liste. Si un seul mot-clé est détecté, son score doit être supérieur au seuil défini. Si plusieurs mots-clés sont détectés, leur score combiné doit être supérieur au seuil défini. Attribuez à chaque mot-clé un score de 1 à 10. Un terme ou une phrase à haute confidentialité, comme « augmentation des salaires » pour le département des ressources humaines, doit avoir un score relativement élevé. Les termes ou les phrases qui, en elles-mêmes, n'ont pas de poids significatif peuvent avoir des scores plus faibles. Pensez aux scores que vous avez attribués aux mots-clés lorsque vous configurez le seuil. Par exemple, si vous avez cinq mots-clés, dont trois avec une priorité élevée, le seuil peut être égal ou inférieur au score combiné des trois mots-clés à priorité élevée. Cela signifie que la détection de ces trois mots-clés est suffisante pour classer le fichier comme étant sensible.

Création d'une liste Mot-clé

Procédure

1. Accédez à **Prévention contre la perte de données** > **Identificateurs de données**.
2. Cliquez sur l'onglet **Mot-clé**.
3. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.
4. Entrez un nom pour la liste de mots-clés. La longueur du nom ne doit pas être supérieure à 100 octets. Le nom ne peut pas contenir les caractères suivants :
   - > < * ^ | & ? \ /
5. Saisissez une description ne dépassant pas 256 octets.
6. Choisissez l'un des critères suivants, puis configurez des paramètres complémentaires pour ce critère :

- **N'importe quel mot-clé**
- **Tous les mots-clés**
- **Tous les mots-clés de <x> caractères maximum**
- **Le score combiné des mots-clés dépasse le seuil**

7. Pour ajouter manuellement des mots-clés à la liste :

a. Saisissez un mot-clé d'une longueur de 3 à 40 octets et indiquez s'il respecte la casse.

b. Cliquez sur **Ajouter**.

8. Pour ajouter des mots-clés à l'aide de l'option d'« importation » :



Remarque

Si le formatage du fichier `.csv` contenant les mots-clés est approprié, utilisez cette option. Pour générer le fichier, vous pouvez exporter les mots-clés à partir du serveur actif ou à partir de tout autre serveur.

a. Cliquez sur **Importer** et identifiez le fichier `.csv` contenant les mots-clés.

b. Cliquez sur **Ouvrir**.

Un message s'affiche et vous informe de la réussite ou de l'échec de l'importation. Si un mot-clé à importer existe déjà dans la liste, il sera ignoré.

9. Pour supprimer des mots-clés, sélectionnez-les puis cliquez sur **Supprimer**.

10. Pour exporter des mots-clés :



Remarque

Utilisez la fonctionnalité « exporter » pour sauvegarder les mots-clés ou les importer sur un autre serveur. Tous les mots-clés de la liste seront exportés. Il n'est pas possible d'exporter un mot-clé individuel.

a. Cliquez sur **Exporter**.

b. Enregistrez le fichier `.csv` obtenu à l'emplacement de votre choix.

11. Cliquez sur **Enregistrer**.

12. Un message s'affiche, vous rappelant de déployer les paramètres vers les agents. Cliquez sur **Fermer**.

13. Lorsque vous êtes à nouveau sur l'écran **Identificateurs de données DLP**, cliquez sur **Appliquer à tous les agents**.

Importation d'une liste Mot-clé

Utilisez cette option si vous avez un fichier `.dat` correctement formaté et contenant les listes de mots-clés. Pour générer le fichier, vous pouvez exporter les listes de mots-clés à partir du serveur actif ou à partir de tout autre serveur.



Remarque

Les fichiers de listes de mots-clés `.dat` générés par cette version de la prévention contre la perte de données ne sont pas compatibles avec les versions précédentes.

Procédure

1. Accédez à **Prévention contre la perte de données** > **Identificateurs de données**.

2. Cliquez sur l'onglet **Mot-clé**.

3. Cliquez sur **Importer** et identifiez le fichier `.dat` contenant les listes de mots-clés.

4. Cliquez sur **Ouvrir**.

   Un message s'affiche et vous informe de la réussite ou de l'échec de l'importation. Si une liste de mots-clés à importer existe déjà, elle sera ignorée.

5. Cliquez sur **Appliquer à tous les agents**.

Modèles de prévention contre la perte de données

Un modèle DLP réunit les identificateurs de données et les opérateurs logiques (Et, Ou, Sauf) pour former des conditions. Seuls les fichiers ou les données qui satisfont à certaines conditions feront l'objet d'une stratégie de prévention contre la perte des données.

Par exemple, un fichier doit être un fichier Microsoft Word (attribut de fichier) ET doit contenir certains termes légaux (mots-clés) ET doit contenir des numéros d'identification (expressions) afin de devenir une stratégie de « Contrats de travail ». Cette stratégie autorise le personnel des Ressources humaines à imprimer le fichier afin que cette copie soit signée par un employé. La transmission par le biais de tous les autres canaux possibles, tels que le courrier électronique, est bloquée.

Vous pouvez créer vos propres modèles si vous avez configuré des identificateurs de données. Vous pouvez également utiliser des modèles prédéfinis. Pour obtenir des informations détaillées, voir *Modèles DLP personnalisés à la page 10-22* et *Modèles DLP prédéfinis à la page 10-21*.



Remarque

Il n'est pas possible de supprimer un modèle utilisé dans une stratégie de prévention contre la perte des données. Supprimez le modèle de la stratégie pour pouvoir la supprimer.

Modèles DLP prédéfinis

La prévention contre la perte de données est fournie avec un ensemble de modèles prédéfinis que vous pouvez utiliser afin de répondre à diverses normes de contrôle. Ces modèles ne peuvent pas être modifiés ou supprimés.

- **GLBA** : Loi Gramm-Leach-Billey Act
- **HIPAA** : Loi Health Insurance Portability and Accountability Act
- **PCI-DSS** : Norme de sécurité des données pour l'industrie des cartes de paiement
- **SB-1386** : Loi n°1386 du Sénat américain

- **US PII** : Données d'identification personnelles des Etats-Unis

Pour obtenir une liste détaillée de tous les modèles prédéfinis, avec des exemples de données sous protection, consultez le document *Listes de protection des données* à l'adresse http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Modèles DLP personnalisés

Créez vos propres modèles si vous avez configuré les identificateurs de données. Un modèle réunit des identificateurs de données et des opérateurs logiques (Et, Ou, Sauf) pour former des déclarations de condition.

Pour plus d'informations et d'exemples sur le fonctionnement des déclarations de condition et des opérateurs logiques, voir *Conditions et opérateurs logiques à la page 10-22*.

Conditions et opérateurs logiques

La prévention contre la perte de données évalue les déclarations de condition de gauche à droite. Lorsque vous configurez des conditions, utilisez les opérateurs logiques avec précaution. Toute utilisation incorrecte génère des conditions erronées, susceptibles de produire des résultats inattendus.

Reportez-vous aux exemples dans le tableau ci-dessous.

TABLEAU 10-4. Exemples de conditions

CONDITION	INTERPRÉTATION ET EXEMPLE
[Identificateur de données 1] **et** [Identificateur de données 2] **sauf** [Identificateur de données 3]	Un fichier doit satisfaire [Identificateur de données 1] et [Identificateur de données 2], mais pas [Identificateur de données 3]. Par exemple : Un fichier doit être [au format Adobe PDF] et doit contenir [une adresse e-mail], mais ne doit pas contenir [tous les mots-clés de la liste].

Condition	Interprétation et exemple
[Identificateur de données 1] **ou** [Identificateur de données 2]	Un fichier doit safisfaire [Identificateur de données 1] ou [Identificateur de données 2]. Par exemple : Un fichier doit être [un document Adobe PDF] ou [un document Microsoft Word].
Sauf [Identificateur de données 1]	Un fichier ne doit pas satisfaire [Identificateur de données 1]. Par exemple : Un fichier ne doit pas être [un fichier multimédia].

Comme illustré dans le dernier exemple du tableau, le premier identificateur de données de la déclaration de condition peut être associé à l'opérateur « sauf » si un fichier ne satisfait pas tous les identificateurs de données dans la décalaration. Cependant, dans la plupart des cas, le premier identificateur de données ne comporte pas d'opérateur.

Création d'un modèle

Procédure

1. Accédez à **Prévention contre la perte de données** > **Modèles DLP**.

2. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.

3. Entrez un nom pour le modèle. La longueur du nom ne doit pas être supérieure à 100 octets. Le nom ne peut pas contenir les caractères suivants :

   - > < * ^ | & ? \ /

4. Saisissez une description ne dépassant pas 256 octets.

5. Sélectionnez des identificateurs de données puis cliquez sur l'icône « Ajouter ».

   Lorsque vous sélectionnez des définitions :

- Sélectionnez plusieurs entrées en appuyant et en maintenant la touche CTRL, puis en sélectionnant les identificateurs de données.
- Si vous recherchez une définition spécifique, utilisez la fonction de recherche. Vous pouvez saisir le nom complet ou partiel de l'identitificateur de données.
- Chaque modèle peut contenir au maximum 40 identificateurs de données.

6. Pour créer une nouvelle expression, cliquez sur **expressions** puis sur **Ajouter une nouvelle expression**. Dans l'écran qui s'affiche, configurez les paramètres de l'expression.
7. Pour créer une nouvelle liste d'attributs, cliquez sur **attributs de fichier** puis sur **Ajouter un nouvel attribut de fichier**. Dans l'écran qui s'affiche, configurez les paramètres de la liste d'attributs de fichier.
8. Pour créer une nouvelle liste de mots-clés, cliquez sur **Mots-clés** puis sur **Ajouter un nouveau mot-clé**. Dans l'écran qui s'affiche, configurez les paramètres de la liste de mots-clés.
9. Si vous avez sélectionné une expression, saisissez le nombre d'occurrences, c'est-à-dire le nombre de fois qu'une expression doit se produire avant que la prévention contre la perte de données ne la soumette à une stratégie.
10. Choisissez un opérateur logique pour chaque définition.



Remarque

Lorsque vous configurez des conditions, utilisez les opérateurs logiques avec précaution. Toute utilisation incorrecte génère des conditions erronées, susceptibles de produire des résultats inattendus. Pour des exemples d'utilisation correcte, voir *Conditions et opérateurs logiques à la page 10-22*.

11. Pour supprimer un identificateur de données de la liste d'identificateurs sélectionnés, cliquez sur l'icône « corbeille ».
12. Sous **Aperçu**, vérifiez la condition et effectuez des changements s'il ne s'agit pas de la condition souhaitée.
13. Cliquez sur **Enregistrer**.
14. Un message s'affiche, vous rappelant de déployer les paramètres vers les agents. Cliquez sur **Fermer**.

15. Lorsque vous êtes à nouveau sur l'écran **Modèles DLP**, cliquez sur **Appliquer à tous les agents**.

Importation d'un modèle

Utilisez cette option si vous disposez d'un fichier `.dat`correctement formaté comprenant les modèles. Pour générer le fichier, vous pouvez exporter les modèles à partir du serveur actif ou à partir de tout autre serveur.



Remarque

Pour importer des modèles DLP depuis OfficeScan 10.6, importez tout d'abord les identificateurs de données associés (auparavant appelés « définitions »). La prévention contre la perte de données ne peut pas importer de modèles auxquels manquent les identificateurs de données associés.

Procédure

1. Accédez à **Prévention contre la perte de données** > **Modèles DLP**.
2. Cliquez sur **Importer**, puis localisez le fichier `.dat` contenant les modèles.
3. Cliquez sur **Ouvrir**.

   Un message s'affiche et vous informe de la réussite ou de l'échec de l'importation. Si un modèle à importer existe déjà, il sera ignoré.
4. Cliquez sur **Appliquer à tous les agents**.

Canaux DLP

Les utilisateurs peuvent transmettre des informations sensibles par le biais de différents canaux. OfficeScan peut contrôler les canaux suivants :

- **Canaux réseau** : les informations sensibles sont transmises selon des protocoles réseau tels que HTTP et FTP.

- **Canaux système et application** : les informations sensibles sont transmises à l'aide d'applications et de périphériques d'un endpoint local.

Canaux réseau

OfficeScan peut contrôler les transmissions de données via les canaux réseau suivants :

- Clients de messagerie
- FTP
- HTTP et HTTPS
- Applications de messagerie instantanée
- Protocole SMB
- Webmail

Pour déterminer les transmissions de données à contrôler, OfficeScan vérifie l'étendue de transmission. Vous devez la configurer. En fonction de l'étendue sélectionnée, OfficeScan contrôlera toutes les transmissions de données ou uniquement les transmissions effectuées en dehors du réseau local (LAN). Pour plus d'informations sur l'étendue des transmissions, voir *Étendue et cibles de transmission pour les canaux réseau à la page 10-30*.

Clients de messagerie

OfficeScan contrôle les courriers électroniques transmis via divers agents de messagerie. OfficeScan vérifie que l'objet, le corps et les pièces jointes du message ne contiennent pas d'identificateurs de données. Pour obtenir la liste des agents de messagerie pris en charge, consultez le document *Listes de protection des données* à l'adresse :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Le contrôle s'effectue lorsqu'un utilisateur tente d'envoyer un e-mail. Si l'e-mail contient des identificateurs de données, OfficeScan l'autorise ou le bloque.

Vous pouvez définir les domaines de messagerie internes contrôlés et non contrôlés.

- **Domaines de messagerie contrôlés** : Quand OfficeScan détecte un courrier électronique transmis à un domaine contrôlé, il vérifie l'action définie par la stratégie. Selon l'action définie, la transmission est autorisée ou bloquée.



Remarque

Si vous définissez les agents de messagerie comme des canaux contrôlés, un courrier électronique doit correspondre à une stratégie pour être contrôlé. Par contre, un courrier électronique envoyé à un domaine de messagerie contrôlé est automatiquement vérifié, même s'il ne correspond pas à une stratégie.

- **Domaines de messagerie non contrôlés** : OfficeScan autorise immédiatement la transmission d'e-mails envoyés à des domaines non contrôlés.



Remarque

Des transmissions de données effectuées vers des domaines de messagerie non contrôlés et vers des domaines de messagerie contrôlés pour lesquels l'action est définie sur « Contrôler » ont le même résultat, à savoir que la transmission est autorisée. La seule différence réside dans le fait que pour les domaines de messagerie non contrôlés, OfficeScan n'enregistre pas la transmission alors que pour les domaines de messagerie contrôlés, la transmission est toujours enregistrée.

Spécifiez des domaines en utilisant l'un des formats suivants en prenant soin de séparer les domaines par des virgules :

- format X400, tel que /O=Trend/OU=USA, /O=Trend/OU=China
- Domaines de messagerie, comme example.com

Pour les e-mails envoyés via le protocole SMTP, OfficeScan vérifie si le serveur SMTP cible se trouve dans les listes suivantes :

1. Cibles contrôlées
2. Cibles non contrôlées



Remarque

Pour plus d'informations sur les cibles contrôlées et non contrôlées, voir *Définition des cibles contrôlées et non contrôlées à la page 10-40*.

3. Domaines de messagerie contrôlés

4. Domaines de messagerie non contrôlés

Cela signifie que si un courrier électronique est envoyé vers un serveur SMTP se trouvant dans la liste des cibles contrôlées, le courrier est vérifié. Si le serveur SMTP ne se trouve pas dans la liste des cibles contrôlées, OfficeScan vérifie les autres listes.

Pour les courriers électroniques envoyés via d'autres protocoles, OfficeScan ne vérifie que les listes suivantes :

1. Domaines de messagerie contrôlés

2. Domaines de messagerie non contrôlés

FTP

Lorsqu'OfficeScan détecte qu'un client FTP tente de charger des fichiers sur un serveur FTP, il vérifie que les fichiers ne contiennent pas d'identificateurs de données. Aucun fichier n'a été chargé jusqu'à présent. En fonction de la stratégie de prévention contre la perte de données, OfficeScan autorise ou bloque le téléchargement.

Lorsque vous configurez une stratégie qui bloque les chargements de fichiers, tenez compte de ce qui suit :

- Lorsqu'OfficeScan bloque un téléchargement, certains clients FTP tenteront de charger de nouveau les fichiers. Dans ce cas, OfficeScan met fin au client FTP pour empêcher les nouvelles tentatives de téléchargement. Les utilisateurs ne reçoivent pas de notification après l'interruption du client FTP. Informez-les de la situation lorsque vous mettez en œuvre vos stratégies de prévention contre la perte de données.

- Si un fichier à charger écrase un fichier du serveur FTP, le fichier du serveur FTP peut être supprimé.

Pour obtenir la liste des clients FTP pris en charge, consultez le document *Listes de protection des données* à l'adresse :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

HTTP et HTTPS

OfficeScan contrôle les données à transmettre via HTTP et HTTPS. Pour HTTPS, OfficeScan vérifie les données avant qu'elles ne soient encodées et transmises.

Pour obtenir la liste des applications et des navigateurs Web pris en charge, consultez le document *Listes de protection des données* à l'adresse :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Applications de messagerie instantanée

OfficeScan contrôle les messages et les fichiers que les utilisateurs envoient via les applications de messagerie instantanée. Les messages et les fichiers reçus par les utilisateurs ne sont pas contrôlés.

Pour obtenir la liste des applications de messagerie instantanée prises en charge, consultez le document *Listes de protection des données* à l'adresse :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Lorsque OfficeScan bloque un message ou un fichier envoyé via AOL Instant Messenger, MSN, Windows Messenger ou Windows Live Messenger, il met également fin à l'application. Si OfficeScan ne ferme pas l'application, celle-ci ne répondra plus et les utilisateurs devront tout de même y mettre fin. Les utilisateurs ne reçoivent pas de notification après la fermeture de l'application. Informez-les de la situation lorsque vous mettez en œuvre vos stratégies de prévention contre la perte de données.

Protocole SMB

OfficeScan contrôle les transmissions de données via le protocole SMB (Server Message Block), qui facilite l'accès aux fichiers partagés. Lorsqu'un autre utilisateur tente de copier ou de lire un fichier partagé par un autre utilisateur, OfficeScan vérifie si le fichier est ou contient un identificateur de données, puis autorise ou bloque l'opération.



Remarque

L'action Contrôle des dispositifs est prioritaire par rapport à l'action de la prévention contre la perte de données. Par exemple, si le contrôle des dispositifs n'autorise pas le déplacement de fichiers sur des lecteurs réseau mappés, la transmission de données sensibles n'aura pas lieu même si la prévention contre la perte de données l'autorise. Pour plus d'informations concernant les actions de contrôle des dispositifs, voir *Autorisations pour les périphériques de stockage à la page 9-4*.

Pour obtenir la liste des applications qu'OfficeScan surveille pour l'accès aux fichiers partagés, consultez le document *Listes de protection des données* à l'adresse :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Webmail

Les services de messagerie Web transmettent les données via HTTP. Si OfficeScan détecte des données sortant des dispositifs pris en charge, il vérifie les données à la recherche d'identificateurs de données.

Pour obtenir la liste des services de messagerie Web pris en charge, consultez le document *Listes de protection des données* à l'adresse :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Étendue et cibles de transmission pour les canaux réseau

L'étendue et les cibles de transmission définissent les transmissions de données sur les canaux réseau qu'OfficeScan doit contrôler. Pour les transmissions qui doivent être contrôlées, OfficeScan vérifie la présence d'identificateurs de données avant d'autoriser ou de bloquer la transmission. Pour les transmissions qui ne doivent pas être contrôlées, OfficeScan ne vérifie pas la présence d'identificateurs de données et autorise directement la transmission.

Étendue de transmission : Toutes les transmissions

OfficeScan contrôle les données transmises hors de l'ordinateur hôte.



Remarque

Trend Micro recommande de choisir cette étendue pour les agents externes.

Si vous ne souhaitez pas contrôler les transmissions de données vers certaines cibles hors de l'ordinateur hôte, définissez les points suivants :

- **Cibles non contrôlées** : OfficeScan ne contrôle pas les données transmises vers ces cibles.



Remarque

Des transmissions de données effectuées vers des cibles non contrôlées et vers des cibles contrôlées pour lesquelles l'action est définie sur « Contrôler » ont le même résultat, à savoir que la transmission est autorisée. La seule différence réside dans le fait que pour les cibles non contrôlées, OfficeScan n'enregistre pas la transmission alors que pour les cibles contrôlées, la transmission est toujours enregistrée.

- **Cibles contrôlées** : il s'agit de cibles spécifiques, au sein des cibles non contrôlées, qui doivent être contrôlées. Les cibles contrôlées sont :
  - facultatives si vous avez défini des cibles non contrôlées.
  - non configurables si vous n'avez pas défini de cibles non contrôlées.

Par exemple :

Les adresses IP suivantes sont attribuées au département juridique de votre entreprise :

- 10.201.168.1 à 10.201.168.25

Vous créez une stratégie qui contrôle la transmission des contrats de travail vers tous les employés à l'exception du personnel travaillant à plein-temps dans le département juridique. Vous devez donc sélectionner **Toutes les transmissions** comme étendue de transmission et ensuite :

Option n°1 :

1. Ajouter 10.201.168.1 à 10.201.168.25 aux cibles non contrôlées.
2. Ajouter les adresses IP du personnel travaillant à temps partiel dans le département juridique aux cibles contrôlées. Il y aurait 3 adresses IP : 10.201.168.21 à 10.201.168.23.

Option n°2 :

Ajouter les adresses IP du personnel travaillant à temps plein dans le département juridique aux cibles non contrôlées.

- 10.201.168.1-10.201.168.20
- 10.201.168.24-10.201.168.25

Pour obtenir les directives sur la manière de définir des cibles contrôlées et non contrôlées, voir *Définition des cibles contrôlées et non contrôlées à la page 10-40*.

Étendue de transmission : uniquement les transmissions hors du réseau local

OfficeScan surveille les données transmises vers une cible hors du réseau local (LAN).



Remarque

Trend Micro recommande de choisir cette étendue pour les agents internes.

« Réseau » se rapporte à l'entreprise ou au réseau local. Cela comprend le réseau actuel (adresse IP du endpoint et masque de réseau) et les adresses IP privées standards suivantes :

- Classe A : 10.0.0.0 à 10.255.255.255
- Classe B : 172.16.0.0 à 172.31.255.255
- Classe C : 192.168.0.0 à 192.168.255.255

Si vous sélectionnez cette étendue de transmission, vous pouvez définir ce qui suit :

- **Cibles non contrôlées** : cibles situées hors du réseau local que vous considérez comme inoffensives et qui ne doivent donc pas être contrôlées.



Remarque

Des transmissions de données effectuées vers des cibles non contrôlées et vers des cibles contrôlées pour lesquelles l'action est définie sur « Contrôler » ont le même résultat, à savoir que la transmission est autorisée. La seule différence réside dans le fait que pour les cibles non contrôlées, OfficeScan n'enregistre pas la transmission alors que pour les cibles contrôlées, la transmission est toujours enregistrée.

- **Cibles contrôlées** : cibles du réseau local que vous souhaitez contrôler.

Pour obtenir les directives sur la manière de définir des cibles contrôlées et non contrôlées, voir *Définition des cibles contrôlées et non contrôlées à la page 10-40*.

Résoudre des conflits

Si les paramètres d'étendue de transmission, de cibles contrôlées et non contrôlées entrent en conflit, OfficeScan applique les priorités suivantes de la plus haute à la plus basse :

- Cibles contrôlées
- Cibles non contrôlées
- Étendue de transmission

Canaux système et application

OfficeScan peut contrôler les canaux système et application suivants :

- Stockage en ligne
- Enregistreurs de données (CD/DVD)
- Applications pair-à-pair
- Cryptage PGP
- Imprimante
- Stockage amovible
- Logiciel de synchronisation (ActiveSync)

- Presse-papiers Windows

Stockage en ligne

OfficeScan contrôle les fichiers auxquels accèdent les utilisateurs via des sources de stockage en ligne. Pour obtenir la liste des sources de stockage en ligne prises en charge, consultez le document *Listes de protection des données* à l'adresse :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Enregistreurs de données (CD/DVD)

OfficeScan contrôle les données enregistrées sur un CD ou un DVD. Pour obtenir la liste des logiciels et des dispositifs d'enregistrement de données pris en charge, consultez le document *Listes de protection des données* à l'adresse :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Lorsque OfficeScan détecte une demande de « gravure » lancée par l'un de ces dispositifs ou logiciels pris en charge et que l'action est « Ignorer », l'enregistrement des données es effectué. Si l'action définie est « Bloquer », OfficeScan vérifie si les fichiers à enregistrer sont ou contiennent des identificateurs de données. Si OfficeScan détecte au moins un identificateur de données, aucun fichier ne sera enregistré, pas même ceux qui ne sont pas des identificateurs de données ou qui n'en contiennent pas. OfficeScan peut également empêcher d'éjecter le CD ou le DVD. Dans ce cas, invitez les utilisateurs à redémarrer le processus logiciel ou à réinitialiser l'ordinateur.

OfficeScan applique des règles d'enregistrement sur CD/DVD supplémentaires :

- Pour limiter les faux positifs, OfficeScan ne contrôle pas les fichiers suivants :

.bud	.dll	.gif	.gpd	.htm	.ico	.ini
.jpg	.lnk	.sys	.ttf	.url	.xml	

- Afin d'améliorer les performances, deux types de fichiers utilisés par les enregistreurs de données Roxio (`*.png` et `*.skn`) ne sont pas contrôlés.

- OfficeScan ne contrôle pas les fichiers des répertoires suivants :

`*:\autoexec.bat`	`*:\Windows`
`..\Application Data`	`..\Cookies`
`..\Local Settings`	`..\ProgramData`
`..\Program Files`	`..\Users\*\AppData`
`..\WINNT`	

- Les images ISO créées par les dispositifs et logiciels ne sont pas contrôlées.

Applications Pair-à-Pair

OfficeScan contrôle les fichiers que les utilisateurs partagent via des applications pair-à-pair.

Pour obtenir la liste des applications pair-à-pair prises en charge, consultez le document *Listes de protection des données* à l'adresse :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Cryptage PGP

OfficeScan contrôle les données à encoder par les logiciels de cryptage PGP. OfficeScan vérifie les données avant le chiffremente.

Pour obtenir la liste des logiciels de cryptage PGP pris en charge, consultez le document *Listes de protection des données* à l'adresse :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Imprimante

OfficeScan contrôle les opérations d'impression lancées depuis diverses applications.

OfficeScan ne bloque pas les opérations d'impression des nouveaux fichiers n'ayant pas été enregistrés, car les informations d'impression n'ont été jusque-là stockées que dans la mémoire.

Pour obtenir la liste des applications prises en charge pouvant lancer des opérations d'impression, consultez le document *Listes de protection des données* à l'adresse :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Stockage amovible

OfficeScan contrôle les transmissions de données vers et au sein des périphériques de stockage amovibles. Voici des exemples d'activités liées à la transmission de données :

- Création d'un fichier dans le périphérique
- Copie d'un fichier de l'ordinateur hôte sur le périphérique
- Fermeture d'un fichier modifié dans le périphérique
- Modification des informations de fichier (extension du fichier, par exemple) dans le périphérique

Lorsqu'un fichier à transmettre contient un identificateur de données, OfficeScan bloque ou autorise la transmission.



Remarque

L'action Contrôle des dispositifs est prioritaire par rapport à l'action de la prévention contre la perte de données. Si le contrôle des dispositifs n'autorise pas la copie de fichiers vers un périphérique de stockage, par exemple, la transmission des données sensibles n'aura pas lieu même si la prévention contre la perte de données l'autorise. Pour plus d'informations concernant les actions de contrôle des dispositifs, voir *Autorisations pour les périphériques de stockage à la page 9-4*.

Pour obtenir la liste des dispositifs de stockage amovibles et des applications qui facilitent la transmission de données pris en charge, consultez le document *Listes de protection des données* à l'adresse :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

La gestion de la transmission de fichiers vers un périphérique de stockage amovible est un processus simple. Par exemple, un utilisateur qui crée un fichier dans Microsoft Word peut souhaiter l'enregistrer sur une carte SD (peu importe le type du fichier à

enregistrer). Si le fichier contient un identificateur de données ne devant pas être transmis, OfficeScan empêche l'enregistrement du fichier.

Pour la transmission de fichiers au sein du périphérique, OfficeScan sauvegarde le fichier (si sa taille est inférieure ou égale à 75 Mo) sur `%WINDIR%\system32\dgagent\temp` avant de le traiter. OfficeScan supprime le fichier de sauvegarde s'il a autorisé la transmission du fichier. Si OfficeScan a bloqué la transmission, il est possible que le fichier ait été effacé au cours du processus. Dans ce cas, OfficeScan va copier le fichier de sauvegarde dans le dossier contenant le fichier d'origine.

OfficeScan vous autorise à définir des exceptions. OfficeScan autorise toujours les transmissions de données vers ou au sein de ces périphériques. Identifie les périphériques selon leurs fournisseurs et peut également procurer leurs modèles et numéros de série.



Conseil

À l'aide de l'outil Liste de dispositifs, interrogez les dispositifs reliés aux endpoints. L'outil indique, pour chaque périphérique, le nom du fournisseur, le modèle et le numéro de série. Pour obtenir des informations détaillées, consultez la section *Outil Liste de dispositifs à la page 9-14*.

Logiciel de synchronisation (ActiveSync)

OfficeScan contrôle les données transmises à un dispositif mobile par le biais d'un logiciel de synchronisation.

Pour obtenir la liste des logiciels de synchronisation pris en charge, consultez le document *Listes de protection des données* à l'adresse :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Si les données ont une adresse IP source 127.0.0.1 et sont envoyées par les ports 990 ou 5678 (les ports utilisés pour la synchronisation), OfficeScan vérifie si les données sont des identificateurs de données avant d'autoriser ou de bloquer la transmission.

Lorsque OfficeScan bloque un fichier transmis sur le port 990, il se peut qu'un fichier de même nom contenant des caractères malformés soit créé dans le dossier de destination

sur le dispositif amovible. Ceci est dû au fait que des parties du fichier ont été copiées sur le dispositif avant que OfficheScan ne bloque la transmission.

Presse-papiers Windows

OfficeScan contrôle les données à transmettre au presse-papiers Windows avant d'autoriser ou de bloquer la transmission.

OfficeScan peut également contrôler les activités du presse-papiers entre l'ordinateur hôte et VMWare ou Remote Desktop. Le contrôle s'effectue sur l'entité sur laquelle se trouve l'agent OfficeScan. Un agent OfficeScan sur une machine virtuelle VMWare, par exemple, peut empêcher la transmission des données du presse-papiers de la machine virtuelle vers l'ordinateur hôte. De même, un ordinateur hôte sur lequel se trouve un agent OfficeScan peut ne pas copier les données du presse-papiers vers un endpoint atteint via Remote Desktop.

Mesures de prévention contre la perte de données

Lorsque la prévention contre la perte de données détecte la transmission d'identificateurs de données, elle vérifie la stratégie DLP pour les identificateurs de données détectés, puis effectue l'action configurée pour la stratégie.

Le tableau suivant répertorie les actions Prévention contre la perte de données.

TABLEAU 10-5. Mesures de prévention contre la perte de données

ACTION	DESCRIPTION
Actions	
Ignorer	La prévention contre la perte de données autorise et consigne la transmission.
Bloquer	La prévention contre la perte de données bloque et consigne la transmission.
Actions supplémentaires	

ACTION	DESCRIPTION
Notifier l'utilisateur de l'agent	La prévention contre la perte de données affiche un message de notification pour informer l'utilisateur de la transmission de données et si cette dernière est autorisée ou bloquée.
Données d'enregistrement	Indépendamment de l'action principale, la prévention contre la perte de données enregistre les informations sensibles dans le répertoire `<dossier d’installation du client>\DLPLite\Forensic`. Sélectionnez cette action pour évaluer les informations sensibles en cours de marquage par Prévention contre la perte de données. Les informations sensibles enregistrées utilisent trop d'espace disque. De ce fait, Trend Micro recommande fortement de choisir cette option uniquement pour les informations hautement sensibles.
Justification de l'utilisateur **Remarque** Cette option est uniquement disponible lorsque l'action **Bloquer** a été sélectionnée.	La prévention contre la perte de données affiche une boîte de dialogue supplémentaire avant d'exécuter l'action « Bloquer ». L'utilisateur peut forcer le contournement de l'action « Bloquer » en fournissant une explication quant à la sûreté du transfert des données sensibles. Les motifs de justification disponibles sont les suivants : • **Cette action est effectuée dans le cadre d'un processus d'entreprise établi.** • **Ce transfert a été approuvé par mon responsable.** • **Les données contenues dans ce fichier ne sont pas confidentielles.** • **Je n'avais pas connaissance des restrictions d'accès liées à ces données.** • **Autre** : les utilisateurs peuvent fournir une autre explication dans ce champ.

Exceptions de prévention contre la perte de données

Les exceptions DLP s'appliquent à l'intégralité de la stratégie, y compris aux règles définies au sein de la stratégie. La prévention contre la perte de données applique les paramètres d'exception à toutes les transmissions avant de scanner les actifs numériques. Si une transmission correspond à l'une des règles d'exception, la prévention contre la perte de données autorise ou scanne immédiatement cette transmission, selon le type d'exception.

Définition des cibles contrôlées et non contrôlées

Définissez les cibles non contrôlées et contrôlées en fonction de la portée de transmission configurée dans l'onglet **Canal**. Pour obtenir plus d'informations sur la manière de définir des cibles contrôlées et non contrôlées pour **Toutes les transmissions**, consultez *Étendue de transmission : Toutes les transmissions à la page 10-30*. Pour obtenir plus d'informations sur la manière de définir des cibles contrôlées et non contrôlées pour **Uniquement les transmissions effectuées hors du réseau local**, consultez *Étendue de transmission : uniquement les transmissions hors du réseau local à la page 10-32*.

Suivez ces instructions lors de la définition de cibles contrôlées ou non contrôlées :

1. Définissez une cible par :

    - Adresse IP
    - Nom d’hôte
    - FQDN
    - Adresse réseau et masque de sous-réseau, par exemple 10.1.1.1/32



Remarque

Pour le masque de sous-réseau, la prévention contre la perte de données ne prend en charge que les ports de type CIDR (Classless Inter-Domain Routing). Cela signifie que vous pouvez ne saisir qu'un numéro comme 32 au lieu de 255.255.255.0.

2. Pour cibler des canaux spécifiques, incluez la valeur par défaut ou les numéros de port définis par l'entreprise pour ces canaux. Par exemple, le port 21 est généralement utilisé pour le trafic FTP, le port 80 pour HTTP et le port 443 pour HTTPS. Utilisez deux points pour séparer la cible des numéros de port.

3. Vous pouvez également inclure des plages de ports. Pour inclure tous les ports, ignorez la plage de ports.

   Vous trouverez ci-dessous des exemples de cibles avec des numéros de port et des plages de ports :

   - 10.1.1.1:80
   - hôte :5-20
   - host.domain.com:20
   - 10.1.1.1/32:20

4. Séparez les cibles par des virgules.

Règles de décompression

Les fichiers contenus dans des fichiers compressés peuvent être scannés pour déceler la présence d'actifs numériques. Pour déterminer les fichiers à scanner, la prévention contre la perte de données applique les règles suivantes à un fichier compressé :

- La taille d'un fichier décompressé dépasse : __ Mo (1 à 512 Mo)
- Le nombre de couches de compression est supérieur à : __ (1-20)
- Le nombre de fichiers à scanner dépasse : __ (1-2000)

Règle 1 : Taille maximale d'un fichier décompressé

Un fichier compressé, après décompression, ne doit pas dépasser la limite définie.

Exemple : Vous avez défini la limite sur 20 Mo.

Scénario 1: Si la taille d'un fichier `.zip` après décompression est de 30 Mo, aucun fichier contenu dans le fichier `.zip` ne sera scanné. Les deux autres règles ne sont plus vérifiées.

Scénario 2: Si la taille du fichier `my_archive.zip` après décompression est de 10 Mo :

- Si `my_archive.zip` ne contient pas de fichiers compressés, OfficeScan ignore la règle 2 et passe à la règle 3.
- Si `my_archive.zip` contient des fichiers compressés, la taille de l'ensemble des fichiers décompressés ne doit pas dépasser la limite. Par exemple, si `my_archive.zip` contient `AAA.rar`, `BBB.zip` et `EEE.zip`, et si `EEE.zip` contient `222.zip` :

`my_archive.zip`			= 10 Mo après décompression
	`\AAA.rar`		= 25 Mo après décompression
	`\BBB.zip`		= 3 Mo après décompression
	`\EEE.zip`		= 1 Mo après décompression
		`\222.zip`	= 2 Mo après décompression

`my_archive.zip`, `BBB.zip`, `EEE.zip` et `222.zip` seront vérifiés en fonction de la règle 2 car la taille combinée de ces fichiers ne dépasse pas la limite de 20 Mo. `AAA.rar` est ignoré.

Règle 2 : Nombre maximal de couches de compression

Les fichiers compris dans le nombre de couches spécifiées seront marqués pour le scan.

Par exemple :

```
my_archive.zip
                  \BBB.zip          \CCC.xls
                  \DDD.txt
                  \EEE.zip          \111.pdf
                                    \222.zip          \333.txt
```

Si vous définissez la limite à deux couches :

- OfficeScan ignore le fichier `333.txt` car il se trouve sur la troisième couche.
- OfficeScan indiquera les fichiers suivants pour le scan et vérifiera la règle 3 :
    - `DDD.txt` (sur la première couche)
    - `CCC.xls` (sur la deuxième couche)
    - `111.pdf` (sur la deuxième couche)

Règle 3 : Nombre maximal de fichiers à scanner

OfficeScan effectuera le scan des fichiers jusqu'à la limite indiquée. OfficeScan effectue le scan des fichiers et des dossiers dans l'ordre numérique, puis dans l'ordre alphabétique.

Reprenons l'exemple de la règle 2, OfficeScan a indiqué les fichiers mis en surbrillance pour le scan :

```
my_archive.zip
                    \BBB.zip            \CCC.xls
                    \DDD.txt
                    \EEE.zip            \111.pdf
                                        \222.zip            \333.txt
```

En outre, `my_archive.zip` contient un dossier nommé `7Folder`, qui n'a pas été vérifié en fonction de la règle 2. Ce dossier contient `FFF.doc` et `GGG.ppt`. Le nombre total de fichiers à scanner est donc de 5, comme indiqué ci-dessous :

```
my_archive.zip
                    \7Folder            \FFF.doc
                    \7Folder            \GGG.ppt
                    \BBB.zip            \CCC.xls
                    \DDD.txt
```

```
             \EEE.zip        \111.pdf

                             \222.zip        \333.txt
```

Si vous définissez la limite à 4 fichiers, les fichiers suivants seront scannés :

- `FFF.doc`
- `GGG.ppt`
- `CCC.xls`
- `DDD.txt`



Remarque

Pour les fichiers contenant des fichiers imbriqués, OfficeScan extrait le contenu des fichiers imbriqués.

Si le contenu extrait est du texte, le fichier hôte (tel que `123.doc`) et les fichiers imbriqués (tels que `abc.txt` et `xyz.xls`) comptent pour un seul fichier.

Si le contenu extrait n'est pas du texte, le fichier hôte (tel que `123.doc`) et les fichiers imbriqués (tels que `abc.exe`) sont comptés séparément.

Événements qui déclenchent les règles de décompression

Les événements suivants déclenchent les règles de décompression :

TABLEAU 10-6. Événements qui déclenchent les règles de décompression

Un fichier compressé qui doit être transmis correspond à une stratégie et l'action définie sur le fichier compressé est Ignorer (transmettre le fichier).	Par exemple, pour contrôler les fichiers .ZIP que les utilisateurs transmettent, vous avez défini un attribut de fichier (.ZIP), l'avez ajouté à un modèle, utilisé ce modèle dans une stratégie et ensuite défini l'action sur **Ignorer**. **Remarque** Si l'action définie est Bloquer, le fichier compressé n'est pas transmis et il n'est donc pas nécessaire de scanner les fichiers qu'il contient.
Un fichier compressé à transmettre ne correspond pas à une stratégie.	Dans ce cas, OfficeScan soumettra le fichier compressé aux règles de décompression afin de déterminer quels fichiers contenus doivent être scannés pour détecter des actifs numériques et s'il faut transmettre ou pas le fichier compressé dans son intégralité.

Les deux événements ont le même résultat. Quand OfficeScan trouve un fichier compressé :

- Si la règle 1 ne donne pas de résultat, OfficeScan autorise la transmission du fichier compressé dans son intégralité.
- Si la règle 1 donne un résultat, les deux autres règles sont vérifiées. OfficeScan autorise la transmission du fichier compressé dans son intégralité si :
    - Aucun fichier scanné ne correspond à une stratégie.
    - Tous les fichiers scannés correspondent à une stratégie et l'action définie est **Ignorer**.

      La transmission du fichier compressé dans son intégralité est bloquée si au moins un des fichiers scannés correspond à une stratégie et si l'action définie est **Bloquer**.

Configuration de la stratégie de prévention contre la perte de données

Vous pouvez commencer à créer des stratégies Prévention contre la perte de données une fois que vous avez configuré les identificateurs de données et que vous les avez organisés en modèles.

En plus des identificateurs de données et des modèles, vous devez configurer des canaux et des actions lorsque vous créez une stratégie. Pour plus d'informations sur les stratégies, voir *Stratégies de prévention contre la perte de données à la page 10-3*.

Création d'une stratégie de prévention contre la perte de données

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Paramètres DLP**.
4. Pour configurer une stratégie applicable aux agents externes, cliquez sur l'onglet **Agents externes** ; pour configurer une stratégie applicable aux agents internes, cliquez sur **Agents internes**.



Remarque

Au besoin, configurez les paramètres d'emplacement des agents. Les agents utiliseront ces paramètres pour déterminer leur emplacement et appliquer la stratégie de prévention contre la perte de données adéquate. Pour plus de détails, reportez-vous au *Emplacement de l'Endpoint à la page 14-2*.

5. Sélectionnez **Activer la prévention contre la perte de données**.
6. Choisissez l'un des éléments suivants :

- Si vous êtes sur l'onglet **Agents externes**, vous pouvez appliquer tous les paramètres de prévention contre la perte de données aux agents internes en sélectionnant **Appliquer tous les paramètres aux agents internes**.
- Si vous êtes sur l'onglet **Agents internes**, vous pouvez appliquer tous les paramètres de prévention contre la perte de données aux agents externes en sélectionnant **Appliquer tous les paramètres aux agents externes**.

7. Sur l'onglet **Règles**, cliquez sur **Ajouter**.

Une stratégie peut contenir jusqu'à 40 règles.

8. Configurez les paramètres de règle.

Pour plus d'informations sur la création de règles DLP, voir *Création de règles de prévention contre la perte de données à la page 10-48*.

9. Cliquez sur l'onglet **Exceptions** et configurez les paramètres d'exception nécessaires.

Pour plus de détails sur les paramètres d'exception disponibles, consultez *Exceptions de prévention contre la perte de données à la page 10-40*.

10. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :

- **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.
- **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Création de règles de prévention contre la perte de données



Remarque

La prévention contre la perte de données traite les règles et les modèles selon leur ordre de priorité. Si une règle est définie sur « Ignorer », la prévention contre la perte de données traite la règle suivante de la liste. Si une règle est définie sur « Bloquer » ou « Justification de l'utilisateur », la prévention contre la perte de données bloque ou accepte l'action de l'utilisateur et interrompt le traitement de cette règle ou de ce modèle.

Procédure

1. Sélectionnez **Activer cette règle**.
2. Indiquez un nom pour la règle.

   Configurez les paramètres du modèle :
3. Cliquez sur l'onglet **Modèle**.
4. Dans la liste **Modèles disponibles**, sélectionnez des modèles, puis cliquez sur **Ajouter**.

   Lorsque vous sélectionnez des modèles :

   - Sélectionnez plusieurs entrées en cliquant sur les noms de modèle, ce qui met leur nom en surbrillance.
   - Si vous recherchez un modèle spécifique, utilisez la fonction de recherche. Vous pouvez y saisir tout ou partie du nom du modèle.

   Remarque

   Chaque règle contient un maximum de 200 modèles.
5. Si votre modèle favori ne se trouve pas dans la liste des **Modèles disponibles** :

   a. cliquez sur **Ajouter un nouveau modèle**.

      L'écran **Modèles de prévention contre la perte de données** s'affiche.

Pour obtenir des instructions sur l'ajout de modèles dans l'écran **Modèles de prévention contre la perte de données,** consultez *Modèles de prévention contre la perte de données à la page 10-21*.

b. Une fois le modèle créé, sélectionnez-le et cliquez sur **Ajouter**.



Remarque

OfficeScan utilise la règle de première correspondance lors de la vérification des modèles. Cela signifie que si un fichier ou des données correspondent à la définition contenue dans un modèle, OfficeScan arrête ses recherches. La priorité se base sur l'ordre des modèles dans la liste.

Configurez les paramètres du canal :

6. Cliquez sur l'onglet **Canal**.

7. Sélectionnez les canaux pour la règle.

   Pour plus d'informations sur les canaux, voir *Canaux réseau à la page 10-26* et *Canaux système et application à la page 10-33*.

8. Si vous avez sélectionné l'un des canaux réseau, sélectionnez la portée de transmission :

   - **Toutes les transmissions**
   - **Uniquement les transmissions hors du réseau local**

   Pour plus d'informations sur l'étendue de transmission, l'influence de l'étendue de transmission sur les cibles et la manière de définir des cibles correctement, voir *Étendue et cibles de transmission pour les canaux réseau à la page 10-30*.

9. Si vous avez sélectionné **Clients de messagerie** :

   a. Cliquez sur **Exceptions**.

   b. Indiquez les domaines de messagerie internes contrôlés et non contrôlés. Pour plus d'informations sur les domaines de messagerie contrôlés et non contrôlés, voir *Clients de messagerie à la page 10-26*.

10. Si vous avez sélectionné **Stockage amovible** :

a. Cliquez sur **Exceptions**.

b. Ajoutez des périphériques de stockage amovibles non contrôlés en les identifiant par leurs fournisseurs. Le modèle et l'ID de série du dispositif sont facultatifs.

La liste approuvée pour les périphériques USB prend en charge l'utilisation de l'astérisque (*) comme caractère générique. Remplacez tout champ avec l'astérisque (*) pour inclure tous les périphériques répondant aux autres champs.

Par exemple, [vendeur]-[modèle]-* place tous les dispositifs USB du vendeur et du type de modèle spécifiés dans la liste approuvée, peu importe l'ID de série.

c. Pour ajouter plusieurs périphériques, cliquez sur l'icône plus (**+**).



Conseil

À l'aide de l'outil Liste de dispositifs, interrogez les dispositifs reliés aux endpoints. L'outil indique, pour chaque périphérique, le nom du fournisseur, le modèle et le numéro de série. Pour obtenir des informations détaillées, consultez la section *Outil Liste de dispositifs à la page 9-14*.

Configurez les paramètres de l'action :

11. Cliquez sur l'onglet **Action**.

12. Sélectionnez une action principale et toute action complémentaire applicable. Pour plus d'informations sur les actions, voir *Mesures de prévention contre la perte de données à la page 10-38*.

13. Après avoir configuré les paramètres de **Modèle**, **Canal** et **Action**, cliquez sur **Enregistrer**.

Importation, Exportation et Copie des règles DLP

Les administrateurs peuvent importer des règles définies précédemment (contenues dans un fichier correctement formaté `.dat`) ou exporter la liste des règles DLP configurées.

Copier une règle DLP permet à un administrateur de modifier le contenu d'une règle précédemment définie afin de gagner du temps.

Le tableau suivant explique le fonctionnement de chaque fonction.

TABLEAU 10-7. Importer, Exporter et Copier les fonctions pour les règles DLP

FONCTION	DESCRIPTION
Importer	Importer une liste de règle permet d'ajouter les règles non existantes à la liste des règles DLP existantes. La prévention contre la perte de données ignore les règles qui existent déjà dans la liste cible. La prévention contre la perte de données conserve tous les paramètres préconfigurés pour chaque règle, y compris l'état activé ou désactivé.
Exporter	L'exportation d'une liste de règles exporte l'intégralité de la liste vers un fichier `.dat`, que les administrateurs peuvent alors importer et déployer sur les autres domaines ou agents. La prévention contre la perte de données enregistre tous les paramètres de règles en fonction de la configuration actuelle. **Remarque** • Les administrateurs doivent enregistrer ou appliquer toute règle nouvelle ou modifiée avant d'exporter la liste. • La prévention contre la perte de données n'exporte aucune exception configurée pour la stratégie, uniquement les paramètres configurés pour chaque règle.
Copier	Copier une règle entraîne la création d'une réplique exacte des paramètres de la configuration actuelle pour la règle. Les administrateurs doivent entrer un nouveau nom pour la règle et peuvent apporter toute modification nécessaire à la configuration pour la nouvelle règle.

Notifications de la prévention contre la perte de données

OfficeScan est fourni avec un ensemble de messages de notification par défaut informant les administrateurs et les utilisateurs des agents OfficeScan des transmissions d'actifs numériques.

Pour plus de détails sur les notifications envoyées aux administrateurs, voir *Notifications de la prévention contre la perte de données pour les administrateurs à la page 10-52*.

Pour plus de détails sur les notifications envoyées aux utilisateurs des agents, voir *Notifications de prévention contre la perte de données pour les utilisateurs des agents à la page 10-56*.

Notifications de la prévention contre la perte de données pour les administrateurs

Configurez OfficeScan afin d'envoyer aux administrateurs une notification lorsqu'il détecte la transmission d'actifs numériques, ou uniquement lorsque la transmission est bloquée.

OfficeScan est fourni avec un ensemble de messages de notification par défaut informant les administrateurs des transmissions d'actifs numériques. Modifiez les notifications et configurez les paramètres de notification supplémentaires pour répondre aux exigences de l'entreprise.



Remarque

OfficeScan peut envoyer des notifications par courrier électronique, déroutement SNMP et via les journaux d'événements de Windows NT. Configurez les paramètres lorsqu'OfficeScan envoie des notifications par le biais de ces chaînes. Pour obtenir des informations détaillées, voir *Paramètres de notification aux administrateurs à la page 13-33*.

Configuration de la notification de prévention contre la perte de données pour les administrateurs

Procédure

1. Accédez à **Administration** > **Notifications** > **Administrateur**.
2. Sous **Critères** l'onglet :
    a. Accédez à la section **Transmissions des actifs numériques**.
    b. Spécifiez si l'envoi des notifications doit être effectué lorsque la transmission d'actifs numériques est détectée (l'action peut être bloquée ou omise) ou uniquement lorsque la transmission est bloquée.
3. Sous **E-mail** l'onglet :
    a. Accédez à la section **Transmissions des actifs numériques**.
    b. Sélectionnez **Activer la notification par courrier électronique**.
    c. Sélectionnez **Envoyer des notifications aux utilisateurs disposant de droits d'accès aux domaines de l'arborescence des agents**.

    Utilisez Role-based Administration afin d'accorder aux utilisateurs l'accès aux domaines de l'arborescence des agents. Si une transmission se produit sur un agent appartenant à un domaine spécifique, le courrier électronique est envoyé aux adresses électroniques des utilisateurs ayant des autorisations sur ce domaine. Pour des exemples, voir le tableau suivant :

TABLEAU 10-8. Domaines et autorisations de l'arborescence des agents

DOMAINE DE L'ARBORESCENCE DES AGENTS	RÔLES AVEC DROITS D'ACCÈS AU DOMAINE	COMPTE UTILISATEUR AVEC LE RÔLE	ADRESSE ÉLECTRONIQUE POUR LE COMPTE UTILISATEUR
Domaine A	Administrateur (intégré)	racine	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
Domaine B	Administrateur (intégré)	racine	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

Si un agent OfficeScan appartenant au domaine A détecte une transmission d'actifs numériques, le courrier électronique sera envoyé à mary@xyz.com, john@xyz.com et chris@xyz.com.

Si un agent OfficeScan appartenant au domaine B détecte la transmission, le courrier électronique est envoyé à mary@xyz.com et jane@xyz.com.



Remarque

Si vous activez cette option, tous les utilisateurs disposant des autorisations sur ce domaine doivent avoir une adresse électronique correspondante. La notification par courrier électronique ne sera pas envoyée aux utilisateurs qui n'ont pas d'adresse électronique. Les utilisateurs et les adresses électroniques sont configurés à partir de **Administration** > **Gestion des comptes** > **Comptes utilisateurs**.

d. Sélectionnez **Envoyer les notifications à/aux (l')adresse(s) électronique(s) suivante(s)**, puis saisissez les adresses électroniques.

e. Acceptez ou modifiez l'objet et le message par défaut. Utilisez des variables de jeton afin de représenter les données dans les champs **Objet** et **Message**.

Tableau 10-9. Variables de jeton pour les notifications de prévention contre la perte de données

Variable	Description
%USER%	Utilisateur connecté au endpoint lors de la détection de la transmission
%COMPUTER%	Endpoint sur lequel la transmission a été détectée
%DOMAIN%	Domaine du endpoint
%DATETIME%	Date et heure auxquelles la transmission a été détectée
%CHANNEL%	Le canal par lequel la transmission a été détectée
%TEMPLATE%	Le modèle d'actifs numériques ayant déclenché la détection
%RULE%	Nom de la règle ayant déclenché la détection

4. Sous l'onglet **Déroutement SNMP** :

   a. Accédez à la section **Transmissions des actifs numériques**.

   b. Sélectionnez **Activer la notification par déroutement SNMP**.

   c. Acceptez ou modifiez le message par défaut. Utilisez des variables de jeton afin de représenter les données dans le champ **Message**. Voir *Tableau 10-9: Variables de jeton pour les notifications de prévention contre la perte de données à la page 10-55* pour plus d'informations.

5. Sous l'onglet **Journal d'événements NT** :

   a. Accédez à la section **Transmissions des actifs numériques**.

   b. Sélectionnez **Activer la notification via le journal d'événements NT**.

   c. Acceptez ou modifiez le message par défaut. Vous pouvez utiliser des variables de jeton afin de représenter les données dans le champ **Message**. Voir *Tableau 10-9: Variables de jeton pour les notifications de prévention contre la perte de données à la page 10-55* pour plus d'informations.

6. Cliquez sur **Enregistrer**.

Notifications de prévention contre la perte de données pour les utilisateurs des agents

OfficeScan peut afficher des messages de notification sur les ordinateurs des agents immédiatement après avoir accepté ou bloqué la transmission d'actifs numériques.

Pour avertir les utilisateurs que la transmission des actifs numériques a été bloquée ou acceptée, sélectionnez l'option **Notifier l'utilisateur de l'agent** lors de la création d'une stratégie de prévention contre la perte de données. Pour obtenir des instructions sur la création d'une stratégie, voir *Configuration de la stratégie de prévention contre la perte de données à la page 10-46*.

Configuration de la notification de prévention contre la perte de données pour les agents

---

Procédure

1. Accédez à **Administration** > **Notifications** > **Agent**.
2. Dans la liste déroulante **Type**, sélectionnez **Transmissions d'actifs numériques**.
3. Acceptez ou modifiez le message par défaut.
4. Cliquez sur **Enregistrer**.

Journaux de prévention contre la perte de données

Les agents consignent les transmissions d'actifs numériques (transmissions bloquées et autorisées) et envoient immédiatement les journaux au serveur. Si l'agent ne parvient pas à envoyer des journaux, un deuxième essai a lieu au bout de 5 minutes.

Pour éviter que les journaux n'occupent trop d'espace sur votre disque dur, vous pouvez les supprimer manuellement ou configurer leur suppression programmée. Voir *Gestion du*

journal à la page 13-36 pour obtenir des informations complémentaires sur la gestion des journaux.

Affichage des journaux de prévention contre la perte de données

Procédure

1. Accédez à **Agents** > **Gestion des agents** ou **Journaux** > **Agents** > **Risques de sécurité**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Journaux** > **Journaux de prévention contre la perte de données** ou **Afficher journaux** > **Journaux DLP**.
4. Spécifiez les critères de journaux, puis cliquez sur **Afficher les journaux**.
5. Affichez les journaux.

   Les journaux contiennent les informations suivantes :

   TABLEAU 10-10. Informations sur les journaux de prévention contre la perte de données

COLONNE	DESCRIPTION
Date et heure	Date et heure de la consignation de l'incident par la prévention contre la perte de données
Utilisateur	Nom de l'utilisateur connecté au endpoint
Endpoint	Nom de l'Endpoint sur lequel la prévention contre la perte de données a détecté la transmission
Domaine	Domaine du endpoint
IP	Adresse IP du endpoint

Colonne	Description
Nom de la règle	Nom de la ou des règles ayant déclenché l'incident **Remarque** Les stratégies créées dans une version précédente d'OfficeScan affichent le nom par défaut LEGACY_DLP_Policy.
Canal	Canal par lequel la transmission s'est produite
Processus	Processus qui a facilité la transmission d'un actif numérique (le processus dépend du canal) Pour obtenir des informations détaillées, consultez la section *Processus par canal à la page 10-58*.
Source	Source du fichier contenant l'actif numérique ou le canal (si aucune source n'est disponible)
Destination	Destination souhaitée du fichier contenant l'actif numérique ou le canal (si aucune source n'est disponible)
Action	Action prise sur la transmission
Détails	Lien qui inclut des informations supplémentaires sur la transmission Pour obtenir des informations détaillées, consultez la section *Détails des journaux de prévention contre la perte de données à la page 10-61*.

6. Pour sauvegarder les journaux dans un fichier CSV (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Processus par canal

Le tableau suivant répertorie les processus qui s'affichent sous la colonne **Processus** des journaux de prévention contre la perte de données.

Tableau 10-11. Processus par canal

Canal	Processus
Logiciel de synchronisation (ActiveSync)	Chemin d'accès complet et nom de processus du logiciel de synchronisation Exemple : `C:\Windows\system32\WUDFHost.exe`
Enregistreur de données (CD/DVD)	Chemin complet et nom de processus de l'enregistreur de données Exemple : `C:\Windows\Explorer.exe`
Presse-papiers Windows	Non applicable
Client de messagerie - Lotus Notes	Chemin complet et nom de processus de Lotus Notes Exemple : `C:\Program Files\IBM\Lotus\Notes\nlnotes.exe`
Client de messagerie - Microsoft Outlook	Chemin complet et nom de processus de Microsoft Outlook Exemple : `C:\Program Files\Microsoft Office\Office12\OUTLOOK.EXE`
Client de messagerie - Tous les clients qui utilisent le protocole SMTP	Chemin complet et nom de processus du client de messagerie Exemple : `C:\Program Files\Mozilla Thunderbird\thunderbird.exe`
Stockage amovible	Nom de processus de l'application qui a transmis les données vers le périphérique de stockage ou au sein de celui-ci Exemple : `explorer.exe`

Canal	Processus
FTP	Chemin complet et nom de processus du client FTP Exemple : `D:\Program Files\FileZilla FTP Client\filezilla.exe`
HTTP	« Application HTTP »
HTTPS	Chemin complet et nom de processus du navigateur ou de l'application Exemple : `C:\Program Files\Internet Explorer\iexplore.exe`
Application de messagerie instantanée	Chemin complet et nom de processus de l'application de messagerie instantanée Exemple : `C:\Program Files\Skype\Phone\Skype.exe`
Application de messagerie instantanée - MSN	• Chemin complet et nom de processus de MSN Exemple : `C:\Program Files\Windows Live\Messenger\msnmsgr.exe` • « Application HTTP » si les données sont transmises à partir d'une fenêtre de conversation
Application Pair à pair	Chemin complet et nom de processus de l'application Pair à pair Exemple : `D:\Program Files\BitTorrent\bittorrent.exe`
Cryptage PGP	Chemin complet et nom de processus du logiciel de chiffrement PGP Exemple : `C:\Program Files\PGP Corporation\PGP Desktop\PGPmnApp.exe`

Canal	Processus
Imprimante	Chemin complet et nom de processus de l'application qui a initié une opération d'impression Exemple : `C:\Program Files\Microsoft Office\Office12\ WINWORD.EXE`
Protocole SMB	Chemin complet et nom de processus de l'application à partir de laquelle l'accès aux fichiers partagés (copie ou création d'un nouveau fichier) a été effectué Exemple : `C:\Windows\Explorer.exe`
Webmail (mode HTTP)	« Application HTTP »
Webmail (mode HTTPS)	Chemin complet et nom de processus du navigateur ou de l'application Exemple : `C:\Program Files\Mozilla Firefox\firefox.exe`

Détails des journaux de prévention contre la perte de données

L'écran **Détails des journaux de prévention contre la perte de données** affiche des informations supplémentaires sur la transmission des actifs numériques. Les détails d'une transmission varient en fonction du canal et du processus via lequel OfficeScan a détecté l'incident.

Le tableau suivant établit une liste des informations s'affichant.

Tableau 10-12. Détails des journaux de prévention contre la perte de données

Détails	Description
Date et heure	Date et heure de la consignation de l'incident par la prévention contre la perte de données

DÉTAILS	DESCRIPTION
ID de violation	ID unique de l'incident
Utilisateur	Nom de l'utilisateur connecté au endpoint
Endpoint	Nom de l'Endpoint sur lequel la prévention contre la perte de données a détecté la transmission
Domaine	Domaine du endpoint
IP	Adresse IP du endpoint
Canal	Canal par lequel la transmission s'est produite
Processus	Processus qui a facilité la transmission d'un actif numérique (le processus dépend du canal) Pour obtenir des informations détaillées, consultez la section *Processus par canal à la page 10-58*.
Source	Source du fichier contenant l'actif numérique ou le canal (si aucune source n'est disponible)
Expéditeur du courrier électronique	Adresse e-mail à partir de laquelle la transmission est partie
Objet du courrier électronique	Ligne de l'objet de l'e-mail contenant l'actif numérique
Destinataire du courrier électronique	Adresses de destination de l'e-mail
URL	URL d'un site Web ou d'une page Web
Utilisateur FTP	Nom d'utilisateur utilisé pour la connexion au serveur FTP
Classe de fichier	Type de fichier dans lequel la prévention contre la perte de données a détecté l'actif numérique

DÉTAILS	DESCRIPTION
Règle/modèle	Liste des noms et modèles de règles exacts qui ont déclenché la détection **Remarque** Chaque règle peut contenir plusieurs modèles ayant déclenché l'incident. Plusieurs noms de modèles sont séparés par des virgules.
Action	Action prise sur la transmission
Motif de justification de l'utilisateur	Motif fourni par l'utilisateur pour justifier le transfert des données sensibles

Activation de la journalisation de débogage pour le module Protection des données

Procédure

1. Obtenez le fichier `logger.cfg` auprès de votre service d'assistance.
2. Ajoutez les données suivantes dans `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\DlpLite`:
    - **Type** : `chaîne`
    - **Nom** : `debugcfg`
    - **Valeur** : `C:\Log\logger.cfg`
3. Créez un dossier intitulé « Log » dans le `C:\ directory`.
4. Copiez le fichier `logger.cfg` dans le dossier « Log ».
5. Déployez la prévention contre la perte des données et les paramètres de contrôle des dispositifs depuis la console Web pour lancer la collecte de journaux.



Remarque

Désactivez la journalisation de débogage pour le module Protection des données en supprimant `debugcfg` dans la clé de Registre et en redémarrant le endpoint.



Chapitre 11

Protection des ordinateurs contre les menaces Internet

Ce chapitre décrit les menaces provenant d'Internet et l'utilisation de OfficeScan pour protéger votre réseau et vos ordinateurs des menaces provenant d'Internet.

Les rubriques sont les suivantes :

À propos des menaces Internet

Les menaces Internet comprennent un large éventail de menaces provenant du Web. Les menaces Internet emploient des méthodes très sophistiquées : au lieu d'utiliser une seule approche ou un seul fichier, elles associent plusieurs techniques et fichiers. Par exemple, les auteurs de menaces Internet modifient constamment la version ou la variante utilisée. Étant donné qu'une menace Internet se trouve à un emplacement défini sur un site Web plutôt que sur un endpoint infecté, l'auteur de cette menace Internet modifie constamment son code pour éviter qu'elle ne soit détectée.

Au cours de ces dernières années, les individus que l'on qualifiait auparavant de pirates, auteurs de virus, spammeurs et créateurs de spywares sont désormais connus sous le nom de cybercriminels. Ces individus utilisent les menaces Internet pour poursuivre deux objectifs. Le premier est de dérober des informations pour les revendre ensuite. Il en résulte une divulgation d'informations confidentielles et une perte d'identité. Le endpoint infecté peut également devenir un vecteur pour transmettre des attaques de phishing ou d'autres activités d'interception d'informations. Entre autres, cette menace risque d'entamer la confiance dans le commerce en ligne et l'économie numérique. Le second objectif est de pirater la puissance de l'processeur d'un utilisateur et de l'utiliser comme instrument pour mener des activités lucratives. Ces activités incluent l'envoi de spam ou l'escroquerie sous la forme d'attaques distribuées de refus de service ou d'activités facturées au clic.

Services d'alerte de contact Command & Control

Les services d'alerte de contact Trend Micro Command & Control (C&C) proposent des capacités de détection et d'alerte améliorées pour atténuer les dégâts causés par des menaces persistantes avancées et des attaques ciblées. Les services d'alerte de contact C&C s'intègrent aux services de réputation de sites Web, ce qui détermine les mesures prises sur les adresses de rappel détectées en fonction du niveau de sécurité de la réputation de sites Web.

La liste d'adresses IP C&C améliore encore plus la détection des rappels C&C à l'aide du moteur d'inspection du contenu réseau afin d'identifier les contacts C&C via n'importe quel canal réseau.

Pour plus d'informations sur la configuration du niveau de sécurité des Services de réputation de sites Web, veuillez consulter *Configuration de Stratégie de réputation de sites Web à la page 11-6*.

TABLEAU 11-1. Fonctionnalités des services d'alerte de contact C&C

FONCTION	DESCRIPTION
Liste d'Informations globales	Trend Micro Smart Protection Network compile la liste Informations globales à partir de sources du monde entier et les teste puis évalue le niveau de risque de chaque adresse de rappel C&C. Les Services de réputation de sites Web utilisent la liste Informations globales en conjonction avec les scores de réputation pour les sites Web malveillants afin de fournir une sécurité renforcée contre les menaces avancées. Le niveau de sécurité de la Réputation de sites Web détermine l'action prise sur les sites Web malveillants ou sur les serveurs C&C selon les niveaux de risque attribués.
Intégration à Deep Discovery Advisor et liste Virtual Analyzer	Les serveurs Smart Protection Server peuvent s'intégrer à Deep Discovery Advisor afin d'obtenir la liste des serveurs Virtual Analyzer C&C. Virtual Analyzer de Deep Discovery Advisor évalue les risques potentiels dans un environnement sûr et, à l'aide d'une technologie heuristique et de méthodes d'évaluation comportementale avancées, attribue un niveau de risque aux menaces analysées. Virtual Analyzer remplit la liste Virtual Analyzer avec toute menace qui tenterait de se connecter à un éventuel serveur C&C. La liste Virtual Analyzer est très spécifique à l'entreprise et fournit une défense plus personnalisée contre les attaques ciblées. Les serveurs Smart Protection Server récupèrent la liste auprès de Deep Discovery Advisor et permettent de comparer toutes les menaces C&C possibles tant à la liste Informations globales qu'à la liste Virtual Analyzer locale. Pour des informations plus détaillées sur la connexion du serveur Smart Protection Server intégré à Deep Discovery Advisor, veuillez consulter *Configuration des paramètres du serveur Smart Protection Server intégré à la page 4-23*.

Fonction	Description
Service des connexions suspectes	Le service des connexions suspectes gère les listes d'adresses IP C&C globales et définies par l'utilisateur et contrôle le comportement des connexions effectuées par les endpoints vers des serveurs C&C potentiels. Pour obtenir des informations détaillées, voir *Service des connexions suspectes à la page 11-13*.
Notifications de l'administrateur	Les administrateurs peuvent choisir de recevoir des notifications détaillées et personnalisables lors de la détection d'un rappel C&C. Pour obtenir des informations détaillées, consultez la section *Configuration des notifications sur les rappels C&C pour les administrateurs à la page 11-19*.
Notifications du endpoint	Les administrateurs peuvent choisir d'envoyer des notifications détaillées et personnalisables aux utilisateurs finaux après la détection d'un rappel C&C sur un endpoint. Pour obtenir des informations détaillées, consultez la section *Activation des messages de notification sur les menaces Internet à la page 11-17*.
Notifications d'épidémies	Les administrateurs peuvent personnaliser les notifications d'épidémies spécifiques aux événements de rappel C&C et préciser si le déclenchement se produit sur un seul endpoint ou à travers l'ensemble du réseau. Pour obtenir des informations détaillées, consultez la section *Épidémies de rappel C&C à la page 11-22*.
Journaux de rappel C&C	Les journaux fournissent des informations détaillées sur tous les événements de rappel C&C. Pour obtenir des informations détaillées, consultez la section *Affichage des journaux de rappel C&C à la page 11-26*.

Réputation de sites Web

La technologie de réputation de sites Web assure le suivi de la crédibilité des domaines Web en leur attribuant un score de réputation, basé sur des facteurs tels que l'ancienneté

du site Web concerné, l'historique de ses changements d'emplacement et les indications d'activités suspectes mises en lumière par l'analyse de comportement des programmes malveillants. Elle continue ensuite à analyser les sites et à bloquer les utilisateurs tentant d'accéder à ceux qui sont infectés.

Les agents OfficeScan envoient des requêtes aux sources Smart Protection pour déterminer la réputation des sites Web auxquels les utilisateurs tentent d'accéder. La réputation d'un site Web est liée à la stratégie de réputation de sites Web qui est appliquée sur le endpoint. Selon la stratégie utilisée, l'agent OfficeScan bloquera ou autorisera l'accès au site Web.



Remarque

Pour plus d'informations concernant les sources Smart Protection, consultez *Liste des sources Smart Protection à la page 4-26*.

Ajoutez les sites Web que vous considérez sûrs dans la liste des sites approuvés, et ceux que vous considérez dangereux dans la liste des sites bloqués. Lorsqu'un agent OfficeScan détecte l'accès à l'un de ces sites Web, il autorise ou bloque automatiquement l'accès et cesse d'envoyer des requêtes aux sources Smart Protection.

Stratégies de réputation de sites Web

Les stratégies de réputation de sites Web indiquent à OfficeScan de bloquer ou d'autoriser l'accès à un site Web donné.

Vous pouvez configurer des stratégies pour les agents internes et externes. Les administrateurs OfficeScan configurent généralement une stratégie plus stricte pour les agents externes.

Les stratégies sont des paramètres détaillés dans l'arborescence des agents OfficeScan. Vous pouvez appliquer des stratégies spécifiques à des groupes d'agents ou à des agents individuels. Vous pouvez également appliquer une stratégie unique à tous les agents.

Une fois que vous avez déployé les stratégies, les agents utilisent les critères d'emplacement définis dans l'écran **Emplacement de l'Endpoint (voir**)*Emplacement de*

l'Endpoint à la page 14-2 afin de déterminer leur emplacement et la stratégie à appliquer. Les agents changent de stratégie à chaque fois que l'emplacement change.

Configuration de Stratégie de réputation de sites Web

Avant de commencer

Spécifiez les informations d'authentification du serveur proxy si vous avez défini un serveur proxy pour gérer la communication HTTP dans votre entreprise et si une authentification est requise avant que l'accès au Web ne soit autorisé.

Pour plus de détails sur la configuration des paramètres de proxy, reportez-vous à *Proxy externe pour les agents OfficeScan à la page 14-52*.

Procédure

1. Accédez à **Agents** > **Gestion des agents**.

2. Sélectionnez les cibles dans l'arborescence des agents.

   - Pour configurer une stratégie pour les agents fonctionnant sous Windows XP, Vista, Windows 7, 8 ou 8.1, sélectionnez l'icône du domaine racine ( ), des domaines ou des agents spécifiques.

     Remarque

     Lorsque vous sélectionnez le domaine racine ou des domaines spécifiques, le paramètre s'applique uniquement aux agents s'exécutant sous Windows XP, Vista, Windows 7, 8 ou 8.1. Le paramètre ne s'applique pas aux agents s'exécutant sous une plate-forme Windows Server 2003, Windows Server 2008 ni Windows Server 2012, même s'ils appartiennent aux domaines.

   - Pour configurer une stratégie pour les agents fonctionnant sous Windows Server 2003, Windows Server 2008 ou Windows Server 2012, sélectionnez un agent spécifique.

3. Cliquez sur **Paramètres** > **Paramètres de réputation de sites Web**.

4. Pour configurer une stratégie applicable aux agents externes, cliquez sur l'onglet **Agents externes** ; pour configurer une stratégie applicable aux agents internes, cliquez sur **Agents internes**.



Conseil

Au besoin, configurez les paramètres d'emplacement des agents. Ces paramètres permettront aux agents de déterminer leur emplacement et d'appliquer la stratégie de réputation de sites Web appropriée. Pour obtenir des informations détaillées, consultez la section *Emplacement de l'Endpoint à la page 14-2*.

5. Sélectionnez **Activer la stratégie de réputation de sites Web sur les systèmes d'exploitation suivants**. Les systèmes d'exploitation répertoriés dans la fenêtre dépendent des cibles que vous avez sélectionnées à l'étape 1.



Conseil

Trend Micro recommande de désactiver la stratégie de réputation de sites Web pour les agents internes si vous utilisez déjà un produit Trend Micro doté de la fonction de réputation de sites Web, tel qu'InterScan Web Security Virtual Appliance.

Lorsqu'une stratégie de réputation de sites Web est activée :

- Les agents externes envoient des requêtes de réputation de sites Web à Smart Protection Network.
- Les agents internes envoient des requêtes de réputation de sites Web :
    - aux serveurs Smart Protection Server si l'option **Envoyer des requêtes aux serveurs Smart Protection Server** est activée. Pour plus d'informations sur cette option, voir l'étape 7.
    - à Smart Protection Network si l'option **Envoyer des requêtes aux serveurs Smart Protection Server** est désactivée.

6. Sélectionnez **Activer l'évaluation**.



Remarque

En mode d'évaluation, les agents autorisent l'accès à tous les sites Web mais consignent dans des journaux les accès aux sites qui sont censés être bloqués lorsque l'évaluation est désactivée. Le mode d'évaluation de Trend Micro a été conçu pour vous permettre d'évaluer les sites Web et prendre les mesures qui vous semblent appropriées. Par exemple, les sites Web que vous considérez sûrs peuvent être ajoutés à la liste des URL approuvées.

7. Sélectionnez **Vérifier les URL HTTPS**.

   La communication HTTPS utilise des certificats pour identifier les serveurs Web. Les données sont chiffrées pour éviter le vol et l'espionnage. Bien que plus sécurisés, l'accès aux site Web utilisant HTTPS entraîne toujours des risques. Les site compromis, même ceux disposant de certificats valides, peuvent héberger des programmes malveillants et volent des informations personnelles. En outre, les certificats sont assez simples à obtenir, ce qui facilite l'installation de serveurs Web malveillants utilisant HTTPS.

   Activez la vérification des URL HTTPS afin de réduire les risques d'exposition aux sites compromis et malveillants qui utilisent HTTPS. OfficeScan peut surveiller le trafic HTTPS dans les navigateurs suivants :

Tableau 11-2. Navigateurs pris en charge pour le trafic HTTPS

Navigateur	Version
Microsoft Internet Explorer	• 6 avec SP2 ou supérieure • 7.x • 8.x • 9.x • 10.x • 11.x
Mozilla Firefox	3.5 ou ultérieure
Chrome	N/A



Important

- Le scan HTTPS ne prend en charge que les plates-formes Windows 8, Windows 8.1 et Windows 2012 en mode poste de travail.
- Après avoir activé le scan HTTPS pour la première fois sur des agents OfficeScan exécutant Internet Explorer 9, 10 ou 11, les utilisateurs doivent activer le module complémentaire `Classe TmIEPlugInBHO` dans la fenêtre du navigateur avant que le scan HTTPS ne soit opérationnel.

  Pour plus d'informations sur la configuration des paramètres d'Internet Explorer pour la réputation de sites Web, consultez l'article suivant de la Base de connaissances :

  - http://esupport.trendmicro.com/solution/en-us/1060643.aspx

8. Sélectionnez **Ne scanner que les ports HTTP courants** pour restreindre le scan de réputation des sites Web au trafic à travers les ports 80, 81, et 8080. Par défaut, OfficeScan scanne tout le trafic au travers de tous les ports.

9. Sélectionnez **Envoyer des requêtes aux serveurs Smart Protection Server** pour que les agents internes envoient des requêtes de réputation de sites Web aux serveurs Smart Protection Server.

   - Si vous activez cette option :

     - Les agents consultent la liste des sources Smart Protection pour savoir à quels serveurs Smart Protection Server envoyer les requêtes. Pour plus d'informations sur la liste des sources Smart Protection, veuillez consulter *Liste des sources Smart Protection à la page 4-26*.

     - Assurez-vous que des serveurs Smart Protection Servers sont disponibles. Si aucun serveur Smart Protection Server n'est disponible, les agents n'envoient pas de requête à Smart Protection Network. Les seules sources restantes de données de réputation de sites Web pour les agents sont les listes des URL approuvées et bloquées (configurées à l'étape 10).

     - Si vous souhaitez que les agents se connectent aux serveurs Smart Protection Server via un serveur proxy, spécifiez les paramètres proxy dans **Administration** > **Paramètres** > **Proxy >** onglet **Proxy interne**.

    - Veillez à mettre régulièrement à jour les serveurs Smart Protection Server pour que la protection reste efficace.
    - Les agents ne bloqueront pas les sites Web non testés. Les serveurs Smart Protection Servers ne stockent pas les données de réputation de sites Web de ces sites Web.
- Si vous désactivez cette option :
    - Les agents envoient des requêtes de réputation de sites Web à Smart Protection Network. Les ordinateurs des agents doivent disposer d'une connexion Internet pour pouvoir envoyer des requêtes.
    - Si la connexion à Smart Protection Network requiert l'authentification du serveur proxy, indiquez les informations d'authentification en accédant à **Administration** > **Paramètres** > **Proxy >** onglet **Proxy externe** > **Mises à jour du serveur OfficeScan**.
    - Les agents bloqueront les sites Web non testés si vous sélectionnez **Bloquer les pages qui n'ont pas été testées par Trend Micro** à l'étape 9.

10. Sélectionnez l'un des niveaux de sécurité de la fonction de réputation de sites Web : **Élevé**, **Moyen** ou **Faible**



Remarque

Les niveaux de sécurité déterminent si OfficeScan autorise ou bloque l'accès à un URL. Par exemple, si vous définissez le niveau de sécurité sur Faible, OfficeScan ne bloque que les URL qui constituent des menaces Web connues. Lorsque vous définissez un niveau de sécurité supérieur, le taux de détection des menaces Web s'améliore mais la possibilité de faux positifs augmente également.

---

11. Si vous désactivez l'option **Envoyer les requêtes aux serveurs Smart Protection Server** dans l'étape 7, vous pouvez sélectionner **Bloque les pages qui n'ont pas été testées par Trend Micro**.



Remarque

Bien que Trend Micro teste activement la sécurité des pages Web, les utilisateurs peuvent rencontrer des pages non testées lorsqu'ils visitent des sites Web nouveaux ou peu consultés. Le blocage de l'accès aux pages non testées peut améliorer la sécurité, mais il peut également empêcher l'accès à des pages sûres.

12. Sélectionnez **Bloquer les pages contenant un script malveillant** afin d'identifier les exploitations de navigateur Web et les scripts malveillants, tout en empêchant que l'utilisation de ces menaces ne compromette le navigateur Internet.

    OfficeScan utilise à la fois le fichier de signatures de prévention contre l'exploitation du navigateur et le fichier de signatures de l'analyseur de script pour identifier et bloquer les pages Web avant que le système ne soit exposé à une menace.

Tableau 11-3. Navigateurs pris en charge pour la prévention contre l'exploitation du navigateur

Navigateur	Version
Microsoft Internet Explorer	• 7.x • 8.x • 9.x • 10.x • 11.x



Important

La fonctionnalité de prévention contre l'exploitation du navigateur requiert l'activation du service de protection avancé (accédez à **Agents** > **Gestion des agents**, cliquez sur **Paramètres** > **Paramètres des services complémentaires**).

13. Configurez les listes d'approbation et de blocage.



Remarque

La liste approuvée est prioritaire sur la liste bloquée. Lorsqu'une URL correspond à une entrée de la liste des URL approuvées, les agents autorisent toujours l'accès à cette URL, même si elle figure dans la liste des URL bloquées.

a. Sélectionnez **Activer la liste des URL approuvées/bloquées**.

b. Entrez une URL.

Vous pouvez ajouter un caractère générique (*) à tout emplacement dans l'URL.

Par exemple :

- Si vous entrez `www.trendmicro.com/*`, cela signifie que toutes les pages du site Web Trend Micro seront approuvées.
- Si vous entrez `*.trendmicro.com/*`, cela signifie que toutes les pages appartenant à un sous-domaine de trendmicro.com seront approuvées.

Vous pouvez également entrer des URL contenant des adresses IP. Si une URL contient une adresse IPv6, précisez l'adresse entre parenthèses.

c. Cliquez sur **Ajouter à la liste des URL approuvées** ou **Ajouter à la liste des URL bloquées**.

d. Pour exporter la liste dans un fichier `.dat`, cliquez sur **Exporter**, puis sur **Enregistrer**.

e. Si vous avez exporté une liste à partir d'un autre serveur et souhaitez l'importer dans cet écran, cliquez sur **Importer** et localisez le fichier `.dat`. La liste est chargée à l'écran.



Important

La réputation de sites Web n'effectue aucun scan des adresses des listes des éléments bloqués et approuvés.

---

14. Pour soumettre des commentaires relatifs à l'évaluation de réputation de sites Web, cliquez sur **Réévaluer l'URL**. Le système de requête du service d'évaluation de la réputation de sites Web de Trend Micro s'ouvre dans une fenêtre de navigateur.

15. Choisissez d'autoriser ou non l'envoi par l'agent OfficeScan de journaux de réputation de sites Web au serveur. Autorisez les agents à envoyer des journaux si vous souhaitez analyser les URL bloqués par OfficeScan, puis entreprenez l'action appropriée sur les URL dont vous estimez l'accès sans danger.

16. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :

    - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.

    - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Service des connexions suspectes

Le service des connexions suspectes gère les listes d'adresses IP C&C globales et définies par l'utilisateur et contrôle le comportement des connexions effectuées par les endpoints vers des serveurs C&C potentiels.

- Les listes des adresses IP approuvées et bloquées définies par l'utilisateur fournissent un niveau de contrôle supplémentaire sur l'accès des endpoints à des adresses IP spécifiques. Configurez ces listes lorsque vous souhaitez autoriser l'accès à une adresse bloquée par la liste d'adresses IP C&C globale ou bloquer l'accès à une adresse pouvant potentiellement représenter un risque de sécurité.

  Pour obtenir des informations détaillées, consultez la section *Configuration des paramètres des listes globales des adresses IP définies par l'utilisateur à la page 11-14*.

- La liste d'adresses IP C&C globale fonctionne en binôme avec le moteur d'inspection du contenu réseau (NCIE) pour détecter les connexions réseaux avec des serveurs C&C confirmés par Trend Micro. Le NCIE détecte un contact serveur C&C via n'importe quel canal réseau. Le service des connexions suspectes consigne dans des journaux toutes les informations relatives aux connexions à des serveurs de la liste d'adresses IP C&C globale pour évaluation ultérieure.

  Pour plus de détails sur l'activation de la liste d'adresses IP C&C globale, voir *Configuration des paramètres de connexion suspecte à la page 11-15*.

- Lorsqu'un programme malveillant a été détecté sur un endpoint à l'aide de la vérification de correspondance du fichier de signatures de règle de pertinence sur les paquets réseau, le service des connexions suspectes peut approfondir l'étude du comportement de connexion afin de déterminer si un rappel C&C a eu lieu. Lorsqu'un rappel C&C a été détecté, le service des connexions suspectes peut tenter de bloquer et de nettoyer la source de la connexion à l'aide de la technologie GeneriClean.

  Pour obtenir des informations détaillées sur la configuration du service des connexions suspectes, voir *Configuration des paramètres de connexion suspecte à la page 11-15*.

  Pour obtenir des informations détaillées sur GeneriClean, voir *GeneriClean à la page E-5*.

Activez le service des connexions suspectes sur l'écran **Paramètres des services complémentaires** afin de protéger les agents contre les rappels de serveur C&C. Pour obtenir des informations détaillées, consultez la section *Activation ou désactivation des services de l'agent à partir de la console Web à la page 14-9*.

Configuration des paramètres des listes globales des adresses IP définies par l'utilisateur

Les administrateurs peuvent configurer OfficeScan de manière à autoriser, bloquer ou consigner toutes les connexions entre les agents et des adresses IP C&C définies par l'utilisateur.



Remarque

Les listes d'adresses IP définies par l'utilisateur prennent uniquement en charge les adresses IPv4.

Procédure

1. Accédez à **Agents** > **Paramètres de l'agent général**.
2. Accédez à la section **Paramètres de connexion suspecte**.
3. Cliquez sur **Modifier la liste des adresses IP définie par l'utilisateur**.

4. Dans l'onglet **Liste des éléments approuvés** ou **Liste des éléments bloqués**, ajoutez les adresses IP que vous souhaitez surveiller.



Conseil

Vous pouvez configurer OfficeScan de manière à ce qu'il ne consigne que les connexions effectuées vers les adresses de la liste des adresses IP bloquées définie par l'utilisateur. Pour que seules les connexions effectuées vers les adresses de la liste des adresses IP bloquées définie par l'utilisateur soient consignées, voir *Configuration des paramètres de connexion suspecte à la page 11-15*.

a. Cliquez sur **Ajouter**.

b. Sur l'écran qui s'affiche alors, saisissez l'adresse IP, la plage d'adresses IP ou l'adresse IPv4 et le masque de sous-réseau qu'OfficeScan doit surveiller.

c. Cliquez sur **Enregistrer**.

5. Pour supprimer une adresse IP de la liste, cochez la case en regard de cette adresse, puis cliquez sur **Supprimer**.

6. Une fois les listes configurées, cliquez sur **Fermer** pour revenir à l'écran **Paramètres de l'agent général**.

Configuration des paramètres de connexion suspecte

OfficeScan peut consigner dans des journaux toutes les connexions effectuées entre des agents et des adresses de liste d'adresses IP C&C globale. L'écran **Paramètres de connexion suspecte** vous permet également de consigner, sans toutefois refuser, l'accès aux adresses IP configurées dans la liste des adresses IP bloquées définie par l'utilisateur.

OfficeScan peut également surveiller les connexions dues à un botnet ou à une autre menace liée à un programme malveillant. Lorsqu'une menace liée à un programme malveillant a été détectée, OfficeScan peut tenter de nettoyer l'infection.

Procédure

1. Accédez à **Agents** > **Gestion des agents**.

2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.

3. Cliquez sur **Paramètres** > **Paramètres de connexion suspecte**.

   L'écran **Paramètres de connexion suspecte** s'affiche.

4. Activez le paramètre **Consigner les connexions vers les adresses de la liste d'adresses IP C&C globale** afin de surveiller les connexions effectuées vers des serveurs C&C confirmés par Trend Micro. Pour plus d'informations sur la liste d'adresses IP C&C globale, voir *Service des connexions suspectes à la page 11-13*.

   - Pour permettre aux agents de se connecter à des adresses de la liste des adresses IP bloquées définie par l'utilisateur, activez le paramètre **Consigner les accès à des adresses de la liste des adresses IP bloquées définie par l'utilisateur et autoriser l'accès à ces adresses**.



Remarque

Vous devez activer la consignation des connexions réseau pour qu'OfficeScan puisse autoriser l'accès aux adresses de la liste des adresses IP bloquées définie par l'utilisateur.

5. Activez le paramètre **Consigner les connexions à l'aide du système de reconnaissance réseau des programmes malveillants** pour exécuter une vérification de correspondance des fichiers de signatures sur les en-têtes des paquets. OfficeScan consigne toutes les connexions effectuées par des paquets dont les en-têtes correspondent à des menaces liées à des programmes malveillants à l'aide du fichier de signatures de règle de pertinence.

   - Pour permettre à OfficeScan de tenter de nettoyer les connexions effectuées vers des serveurs C&C, activez le paramètre **Nettoyer les connexions suspectes lorsqu'un rappel C&C est détecté**. OfficeScan utilise GeneriClean pour nettoyer la menace liée à un programme malveillant et mettre fin à la connexion au serveur C&C.



Remarque

Vous devez activer **Consigner les connexions à l'aide du système de reconnaissance réseau des programmes malveillants** pour qu'OfficeScan puisse tenter de nettoyer les connexions effectuées vers des serveurs C&C détectées par le processus de vérification de la correspondance de la structure des paquets.

6. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :

   - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Notifications sur les menaces Internet pour les utilisateurs des agents

OfficeScan peut afficher un message de notification sur le endpoint d'un agent OfficeScan immédiatement après avoir bloqué une URL qui viole une stratégie de réputation de sites Web. Il vous faut activer le message de notification et, de façon facultative, modifier son contenu.

Activation des messages de notification sur les menaces Internet

Procédure

1. Accédez à **Agents** > **Gestion des agents**.

2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.

3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.

4. Cliquez sur l'onglet **Autres paramètres**.

5. Dans la section **Paramètres de réputation de sites Web**, sélectionnez **Afficher une notification lorsqu'un site Web est bloqué**.

6. Dans la section **Paramètres de rappel C&C**, sélectionnez **Afficher une notification lorsqu'un rappel C&C est détecté**.

7. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :

   - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.

   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Modification des notifications sur les menaces Internet

Procédure

1. Accédez à **Administration** > **Notifications** > **Agent**.

2. Dans la liste déroulante **Type**, sélectionnez le type de notifications sur les menaces Internet à modifier :

   - **Violations de la réputation de sites Web**

   - **Rappels C&C**

3. Saisissez le message par défaut dans la zone de texte prévue à cet effet.
4. Cliquez sur **Enregistrer**.

Configuration des notifications sur les rappels C&C pour les administrateurs

OfficeScan est fourni avec un ensemble de messages de notification par défaut vous informant, ainsi que les autres administrateurs OfficeScan, des détections de rappels C&C. Vous pouvez modifier les notifications et configurer des paramètres de notification supplémentaires qui répondent à vos exigences.

Procédure

1. Accédez à **Administration** > **Notifications** > **Administrateur**.
2. Sous **Critères** l'onglet :
   a. Accédez à la section **Rappels C&C**.
   b. Spécifiez si l'envoi des notifications doit être effectué lorsqu'OfficeScan détecte un rappel C&C (l'action peut être bloquée ou consignée) ou uniquement lorsque le niveau de risque du rappel est Élevé.
3. Sous **E-mail** l'onglet :
   a. Accédez à la section **Rappels C&C**.
   b. Sélectionnez **Activer la notification par courrier électronique**.
   c. Sélectionnez **Envoyer des notifications aux utilisateurs disposant de droits d'accès aux domaines de l'arborescence des agents**.

      Utilisez Role-based Administration afin d'accorder aux utilisateurs l'accès aux domaines de l'arborescence des agents. Si une transmission se produit sur un agent appartenant à un domaine spécifique, le courrier électronique est envoyé aux adresses électroniques des utilisateurs ayant des autorisations sur ce domaine. Pour des exemples, voir le tableau suivant :

TABLEAU 11-4. Domaines et autorisations de l'arborescence des agents

DOMAINE DE L'ARBORESCENCE DES AGENTS	RÔLES AVEC DROITS D'ACCÈS AU DOMAINE	COMPTE UTILISATEUR AVEC LE RÔLE	ADRESSE ÉLECTRONIQUE POUR LE COMPTE UTILISATEUR
Domaine A	Administrateur (intégré)	racine	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
Domaine B	Administrateur (intégré)	racine	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

Si un agent OfficeScan appartenant au domaine A détecte un rappel C&C, le courrier électronique sera envoyé à mary@xyz.com, john@xyz.com et chris@xyz.com.

Si un agent OfficeScan appartenant au domaine B détecte le rappel C&C, le courrier électronique est envoyé à mary@xyz.com et jane@xyz.com.



Remarque

Si vous activez cette option, tous les utilisateurs disposant des autorisations sur ce domaine doivent avoir une adresse électronique correspondante. La notification par courrier électronique ne sera pas envoyée aux utilisateurs qui n'ont pas d'adresse électronique. Les utilisateurs et les adresses électroniques sont configurés à partir de **Administration** > **Gestion des comptes** > **Comptes utilisateurs**.

d. Sélectionnez **Envoyer les notifications à/aux (l')adresse(s) électronique(s) suivante(s)**, puis saisissez les adresses électroniques.

e. Acceptez ou modifiez l'objet et le message par défaut. Utilisez des variables de jeton afin de représenter les données dans les champs **Objet** et **Message**.

TABLEAU 11-5. Variables de jetons pour les notifications de rappels C&C

VARIABLE	DESCRIPTION
%CLIENTCOMPUTER%	Endpoint cible ayant envoyé le rappel
%IP%	Adresse IP du endpoint ciblé
%DOMAIN%	Domaine de l'ordinateur
%DATETIME%	Date et heure auxquelles la transmission a été détectée
%CALLBACKADDRESS%	Adresse de rappel du serveur C&C
%CNCRISKLEVEL%	Niveau de risque du serveur C&C
%CNCLISTSOURCE%	Indique la liste source C&C
%ACTION%	Mesure prise

4. Sous l'onglet **Déroutement SNMP** :
   a. Accédez à la section **Rappels C&C**.
   b. Sélectionnez **Activer la notification par déroutement SNMP**.
   c. Acceptez ou modifiez le message par défaut. Utilisez des variables de jeton afin de représenter les données dans le champ **Message**. Voir *Tableau 11-5: Variables de jetons pour les notifications de rappels C&C à la page 11-21* pour plus d'informations.
5. Sous l'onglet **Journal d'événements NT** :
   a. Accédez à la section **Rappels C&C**.
   b. Sélectionnez **Activer la notification via le journal d'événements NT**.
   c. Acceptez ou modifiez le message par défaut. Vous pouvez utiliser des variables de jeton afin de représenter les données dans le champ **Message**. Voir *Tableau 11-5: Variables de jetons pour les notifications de rappels C&C à la page 11-21* pour plus d'informations.

6. Cliquez sur **Enregistrer**.

Notifications des alertes de contact C&C pour les utilisateurs des agents

OfficeScan peut afficher un message de notification sur les ordinateurs des agents OfficeScan immédiatement après avoir bloqué une URL du serveur C&C. Vous devez activer le message de notification et, si vous le souhaitez, modifier son contenu.

Épidémies de rappel C&C

Définir une épidémie de rappel C&C par le nombre, la source et le niveau de risque des rappels.

OfficeScan est fourni avec un message de notification par défaut vous informant, ainsi que les autres administrateurs OfficeScan, d'une épidémie. Vous pouvez modifier le message de notification en fonction de vos besoins.



Remarque

OfficeScan peut vous envoyer des notifications d'épidémies de rappel C&C par courrier électronique. Configurez les paramètres de messagerie pour permettre à OfficeScan d'envoyer des e-mails correctement. Pour obtenir des informations détaillées, voir *Paramètres de notification aux administrateurs à la page 13-33*.

Configuration des critères et notifications de l'épidémie de violation des rappels C&C

Procédure

1. Accédez à **Administration** > **Notifications** > **Épidémie**.
2. Dans l'onglet **Critères**, configurez les options suivantes :

OPTION	DESCRIPTION
Même hôte compromis	Sélectionnez cette option pour définir une épidémie sur la base des détections de rappels par endpoint
Niveau de risque C&C	Indiquez si vous souhaitez déclencher une épidémie sur tous les rappels C&C ou uniquement sur les sources à risque élevé
Action	Choisissez parmi **Toute action**, **Consigné** ou **Bloqué**
Détections	Indiquez le nombre de détections qui définit une épidémie
Période	Indiquez l'intervalle d'heures durant lequel le nombre de détections doit avoir lieu



Conseil

Trend Micro recommande d'accepter les valeurs par défaut dans cet écran.

3. Dans l'onglet **Courrier électronique** :

   a. Accédez à la section **Rappels C&C**.

   b. Sélectionnez **Activer la notification par courrier électronique**.

   c. Indiquez les destinataires de l'e-mail.

   d. Acceptez ou modifiez l'objet et le message par défaut de l'e-mail. Vous pouvez utiliser des variables de jeton afin de représenter les données dans les champs **Objet** et **Message**.

   TABLEAU 11-6. Variables de jeton pour les notifications d'épidémie de rappel C&C

VARIABLE	DESCRIPTION
%C	Nombre de journaux de rappel C&C
%T	Période d'accumulation des journaux de rappel C&C

   e. Sélectionnez parmi les informations de rappel C&C supplémentaires à inclure dans le courrier électronique.

4. Dans l'onglet **Déroutement SNMP**.

a. Accédez à la section **Rappels C&C**.

b. Sélectionnez **Activer la notification par déroutement SNMP**.

c. Acceptez ou modifiez le message par défaut. Vous pouvez utiliser des variables de jeton afin de représenter les données dans le champ **Message**. Voir *Tableau 11-6: Variables de jeton pour les notifications d'épidémie de rappel C&C à la page 11-23* pour plus d'informations.

5. Dans l'onglet **Journal des événements NT** :

a. Accédez à la section **Rappels C&C**.

b. Sélectionnez **Activer la notification via le journal d'événements NT**.

c. Acceptez ou modifiez le message par défaut. Vous pouvez utiliser des variables de jeton afin de représenter les données dans le champ **Message**. Voir *Tableau 11-6: Variables de jeton pour les notifications d'épidémie de rappel C&C à la page 11-23* pour plus d'informations.

6. Cliquez sur **Enregistrer**.

Journaux des menaces Web

Configurez les agents internes et externes de façon à ce qu'ils envoient des journaux de réputation de sites Web au serveur. Effectuez cette action si vous souhaitez analyser les URL bloqués par OfficeScan et entreprendre les actions appropriées à l'encontre des URL auxquels vous estimez pouvoir accéder en toute sécurité.

Pour éviter que les journaux n'occupent trop d'espace sur votre disque dur, vous pouvez les supprimer manuellement ou configurer leur suppression programmée. Voir *Gestion du journal à la page 13-36* pour obtenir des informations complémentaires sur la gestion des journaux.

Affichage de journaux de réputation de sites Web

Procédure

1. Accédez à **Journaux** > **Agents** > **Risques de sécurité** ou **Agents** > **Gestion des agents**.

2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.

3. Cliquez sur **Afficher journaux** > **Journaux de réputation de sites Web** ou **Journaux** > **Journaux de réputation de sites Web**.

4. Spécifiez les critères de journaux, puis cliquez sur **Afficher les journaux**.

5. Affichez les journaux. Les journaux contiennent les informations suivantes :

Élément	Description
Date et heure	Moment de la détection
Endpoint	Endpoint sur lequel la détection a eu lieu
Domaine	Domaine du endpoint sur lequel la détection a eu lieu
URL	URL bloquée par les services de réputation de sites Web
Niveau de risque	Niveau de risque de l'adresse URL
Description	Description de la menace de sécurité
Processus	Processus via lequel la tentative de contact a eu lieu (chemin_d'accès\nom_de_l'application)

6. S'il existe des URL qui ne doivent pas être bloquées, cliquez sur le bouton **Ajouter à la liste approuvée** pour ajouter le site Web à la liste des URL approuvées.

7. Pour sauvegarder les journaux dans un fichier `CSV` (valeurs séparées par des virgules), cliquez sur **Tout exporter vers un fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Affichage des journaux de rappel C&C

Procédure

1. Accédez à **Journaux** > **Agents** > **Risques de sécurité** ou **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Afficher les journaux** > **Journaux de rappel C&C** ou **Journaux** > **Journaux de rappel C&C** .
4. Spécifiez les critères de journaux, puis cliquez sur **Afficher les journaux**.
5. Affichez les journaux. Les journaux contiennent les informations suivantes :

Élément	Description
Date et heure	Moment de la détection
Utilisateur	Nom de l'utilisateur connecté au moment de la détection
Hôte compromis	Endpoint d'où provient le rappel
Adresse IP	Adresse IP de l'hôte compromis
Domaine	Domaine du endpoint sur lequel la détection a eu lieu
Adresse de rappel	Adresse à laquelle le endpoint a envoyé le rappel
Source de liste C&C	Source de liste C&C ayant identifié le serveur C&C
Niveau de risque C&C	Niveau de risque du serveur C&C
Protocole	Protocole Internet utilisé pour la transmission
Processus	Processus ayant lancé la transmission (chemin_d'accès\nom_de_l'application)
Action	Action prise sur le rappel

6. Si vous souhaitez que certaines URL ne soient pas bloquées par la réputation de sites Web, cliquez sur le bouton **Ajouter à la liste approuvée par la réputation**

de sites Web pour ajouter l'adresse à la liste des URL approuvées par la réputation de sites Web.



Remarque

OfficeScan peut ajouter l'URL à la liste des URL approuvées par la réputation de sites Web. Pour les détections effectuées par la Liste d'adresses IP C&C globale ou la Liste de Virtual Analyzer (IP) C&C, ajoutez manuellement ces adresses IP à la liste des adresses IP C&C approuvées définie par l'utilisateur.

Pour obtenir des informations détaillées, consultez la section *Configuration des paramètres des listes globales des adresses IP définies par l'utilisateur à la page 11-14*.

7. Pour sauvegarder les journaux dans un fichier `CSV` (valeurs séparées par des virgules), cliquez sur **Tout exporter vers un fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Affichage des journaux des connexions suspectes

Procédure

1. Accédez à **Journaux** > **Agents** > **Risques de sécurité** ou **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Afficher les journaux** > **Journaux des connexions suspectes** ou sur **Journaux** > **Journaux des connexions suspectes**.
4. Spécifiez les critères de journaux, puis cliquez sur **Afficher les journaux**.
5. Affichez les journaux. Les journaux contiennent les informations suivantes :

ÉLÉMENT	DESCRIPTION
Date et heure	Moment de la détection
Endpoint	Endpoint sur lequel la détection a eu lieu

Élément	Description
Domaine	Domaine du endpoint sur lequel la détection a eu lieu
Processus	Processus ayant lancé la transmission (chemin_d'accès\nom_de_l'application)
Adresse IP et port locaux	Adresse IP et numéro de port du endpoint source
Adresse IP et port distants	Adresse IP et numéro de port du endpoint de destination
Résultat	Résultat de l'action entreprise
Détecté par	Source de liste C&C ayant identifié le serveur C&C
Direction du trafic	Direction de la transmission

6. Pour sauvegarder les journaux dans un fichier `CSV` (valeurs séparées par des virgules), cliquez sur **Tout exporter vers un fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.



Chapitre 12

Utilisation du pare-feu OfficeScan

Ce chapitre décrit les fonctionnalités et les configurations du pare-feu OfficeScan.

Les rubriques sont les suivantes :

À propos du pare-feu OfficeScan

Le pare-feu OfficeScan protège les agents et les serveurs du réseau grâce à une fonction « Stateful inspection » et à des scans antivirus de réseau hautes performances. Via la console d'administration centralisée, vous pouvez créer des règles pour filtrer les connexions par application, adresse IP, numéro de port ou protocole, puis appliquer les règles à différents groupes d'utilisateurs.



Remarque

Vous pouvez activer, configurer et utiliser le pare-feu OfficeScan sur des endpoints Windows XP dont le pare-feu Windows est également activé. Cependant, vous devez gérer attentivement vos stratégies pour éviter de créer des stratégies de pare-feu conflictuelles et de produire des résultats inattendus. Consultez la documentation Microsoft pour obtenir des informations détaillées sur le pare-feu Windows.

Le pare-feu OfficeScan inclut les fonctionnalités et améliorations clés suivantes :

- *Filtrage du trafic à la page 12-2*
- *Filtrage d'applications à la page 12-3*
- *Liste Certified Safe Software à la page 12-3*
- *Recherche de virus de réseau à la page 12-4*
- *Profils et stratégies personnalisables à la page 12-4*
- *Stateful Inspection à la page 12-4*
- *Système de détection d'intrusion à la page 12-4*
- *Surveillance des épidémies de violation de pare-feu à la page 12-6*
- *Privilèges de pare-feu des agents OfficeScan à la page 12-6*

Filtrage du trafic

Le pare-feu OfficeScan filtre l'ensemble du trafic entrant et sortant, permettant ainsi de bloquer certains types de trafic sur la base des critères suivants :

- Direction (entrant/sortant)
- Protocole (TCP/UDP/ICMP/ICMPv6)
- Ports de destination
- Endpoints source et de destination

Filtrage d'applications

Le pare-feu OfficeScan filtre le trafic entrant et sortant de certaines applications, permettant à ces dernières d'accéder au réseau. Cependant, les connexions réseau dépendront des stratégies définies par l'administrateur.



Remarque

OfficeScan ne prend pas en charge les exceptions d'applications spécifiques sur les plates-formes Windows 8, Windows 8.1 et Windows Server 2012. OfficeScan autorise ou refuse tout le trafic d'applications sur les endpoints exécutant ces plates-formes.

Liste Certified Safe Software

La liste Certified Safe Software fournit une liste d'applications qui peuvent contourner les niveaux de sécurité de la stratégie de pare-feu. Si le niveau de sécurité est défini à Moyen ou Élevé, OfficeScan permettra tout de même aux applications de s'exécuter et d'accéder au réseau.

Activez l'interrogation de la liste Certified Safe Software globale qui s'avère plus complète. Il s'agit d'une liste que Trend Micro met à jour de manière dynamique.



Remarque

Cette fonctionnalité utilise la surveillance des comportements. Vérifiez que le service de prévention des modifications non autorisées et Certified Safe Software Service ont été activés avant d'activer la liste Liste Certified Safe Software globale.

Recherche de virus de réseau

Le pare-feu OfficeScan vérifie également la présence de virus de réseau dans chaque paquet. Pour obtenir des informations détaillées, voir *Virus et programmes malveillants à la page 7-2*.

Profils et stratégies personnalisables

Le pare-feu OfficeScan vous permet de configurer des stratégies destinées à bloquer ou à autoriser certains types de trafic réseau. Attribuez une stratégie à un ou plusieurs profils, que vous pouvez ensuite déployer sur des agents OfficeScan. Vous disposez ainsi d'une méthode d'organisation et de configuration personnalisée des paramètres de pare-feu des agents.

Stateful Inspection

Le pare-feu OfficeScan est de type « Stateful inspection » : il contrôle toutes les connexions à l'agent OfficeScan et mémorise tous les états de connexion. Il peut identifier les conditions spécifiques de toute connexion, prédire les actions qui doivent être effectuées et détecter toute anomalie de connexion. L'utilisation efficace du pare-feu repose donc non seulement sur la création de profils et de stratégies, mais aussi sur l'analyse des connexions et le filtrage des paquets qui transitent par le pare-feu.

Système de détection d'intrusion

Le pare-feu OfficeScan comprend également un système de détection d'intrusion (SDI). Lorsqu'il est activé, le SDI peut contribuer à identifier des fichiers de signatures dans les paquets réseau, indiquant une attaque de l'agent OfficeScan. Le pare-feu OfficeScan peut empêcher les intrusions bien connues suivantes :

Intrusion	Description
Fragment trop important	Attaque de déni de service dans le cadre de laquelle un pirate dirige un paquet TCP/UDP surdimensionné sur un endpoint cible. Par conséquent, la mémoire tampon du endpoint peut déborder, ce qui risque de bloquer ou de redémarrer le endpoint.

Intrusion	Description
Ping of Death	Attaque de déni de service dans le cadre de laquelle un pirate dirige un paquet ICMP/ICMPv6 surdimensionné sur un endpoint cible. Par conséquent, la mémoire tampon du endpoint peut déborder, ce qui risque de bloquer ou de redémarrer le endpoint.
ARP conflictuel	Type d'attaque dans le cadre de laquelle un pirate envoie à un endpoint ciblé une requête de protocole de résolution d'adresse (Address Resolution Protocol ou ARP) avec des adresses IP source et de destination identiques. Le endpoint cible s'envoie continuellement une réponse ARP (son adresse MAC) et dès lors se bloque ou plante.
SYN Flood	Attaque de déni de service dans le cadre de laquelle un programme envoie plusieurs paquets de synchronisation TCP (SYN) à un endpoint, celui-ci envoyant alors continuellement des réponses d'accusé-réception de synchronisation (SYN/ACK). Cela peut épuiser la mémoire du endpoint et finalement bloquer ce dernier.
Fragment de chevauchement	Similaire à une attaque Teardrop, cette attaque de déni de service envoie des fragments TCP de chevauchement à un endpoint. Par conséquent, les informations de l'en-tête sont écrasées dans le premier fragment TCP qui risque alors de passer à travers le pare-feu. Le pare-feu peut ensuite autoriser les fragments suivants contenant du code malveillant à se frayer un chemin vers le endpoint cible.
Teardrop	Similaire à une attaque de fragment de chevauchement, cette attaque de refus de service a trait à des fragments IP. Une valeur de décalage prêtant à confusion dans le deuxième fragment IP ou dans un fragment ultérieur peut provoquer le blocage du système d'exploitation du endpoint récepteur lorsque celui-ci tente de réassembler les fragments.
attaque par fragment minuscule	Avec ce type d'attaque, un fragment TCP de petite taille force la première en-tête de paquet TCP dans le fragment suivant. Cela peut amener les routeurs filtrant le trafic à ignorer les fragments suivants qui peuvent contenir des données malveillantes.
IGMP fragmenté	Attaque de déni de service qui envoie des paquets d'IGMP fragmentés à un endpoint cible, lequel ne peut pas les traiter correctement. Cela peut bloquer ou ralentir le endpoint.

INTRUSION	DESCRIPTION
attaque LAND	Type d'attaque qui envoie à un endpoint des paquets de synchronisation IP (SYN) dont les adresses source et cible sont identiques. Celui-ci s'envoie alors en retour un accusé-réception de la synchronisation (SYN/ACK). Cela peut bloquer ou ralentir le endpoint.

Surveillance des épidémies de violation de pare-feu

Le pare-feu OfficeScan envoie un message de notification à des destinataires spécifiés lorsque le nombre de violations de pare-feu dépasse un seuil déterminé, ce qui peut constituer un signal d'attaque.

Privilèges de pare-feu des agents OfficeScan

Accordez aux utilisateurs des agents OfficeScan le privilège d'afficher leurs paramètres de pare-feu sur la console de l'agent OfficeScan. Vous pouvez également accorder aux utilisateurs le privilège d'activation ou de désactivation du pare-feu, du système de détection d'intrusion et du message de notification de violation du pare-feu.

Activation ou désactivation du pare-feu OfficeScan

Pendant l'installation du serveur OfficeScan, vous êtes invité à activer ou désactiver le pare-feu OfficeScan.

Si vous avez activé le pare-feu pendant l'installation et remarqué que les performances en avaient été affectées, notamment sur les plates-formes serveur (Windows Server 2003, Windows Server 2008 et Windows Server 2012), désactivez le pare-feu.

Si vous avez désactivé le pare-feu pendant l'installation et que vous souhaitez désormais l'activer afin de protéger l'agent des intrusions, veuillez d'abord lire les indications et instructions dans *Services de l'agent OfficeScan à la page 14-7*.

Vous pouvez activer ou désactiver le pare-feu sur l'ensemble des endpoints des agents OfficeScan ou sur certains d'entre eux.

Activation ou désactivation du pare-feu OfficeScan sur certains endpoints

Utilisez l'une des méthodes suivantes pour activer ou désactiver le pare-feu :

MÉTHODE	PROCÉDURE
Créer une stratégie et l'appliquer aux agents OfficeScan	1. Créez une stratégie qui active/désactive le pare-feu. Pour connaître les étapes de création d'une stratégie, voir *Ajout ou modification d'une stratégie de pare-feu à la page 12-11*. 2. Appliquez la stratégie aux agents OfficeScan.
Activer/Désactiver le pilote et le service de pare-feu	1. Activez/désactivez le pilote de pare-feu. a. Ouvrez les **propriétés de connexion au réseau Windows**. b. Cochez ou décochez la case **Pilote du pare-feu commun Trend Micro** pour la carte réseau. 2. Activez/désactivez le service de pare-feu. a. Ouvrez une invite de commande et entrez `services.msc`. b. Démarrez ou arrêtez le **Pare-feu d'OfficeScan NT** dans Microsoft Management Console (MMC).
Activez/désactivez le service de pare-feu de la console Web	Pour les étapes détaillées, voir *Services de l'agent OfficeScan à la page 14-7*.

Activation ou désactivation du pare-feu OfficeScan sur tous les endpoints

Procédure

1. Accédez à **Administration** > **Paramètres** > **Licence du produit**.
2. Accédez à la section **Services complémentaires**.
3. Dans la section **Services complémentaires**, à côté de la ligne **Pare-feu pour endpoints**, cliquez sur **Activer** ou sur **Désactiver**.

Stratégies et profils de pare-feu

Le pare-feu OfficeScan utilise des stratégies et des profils pour organiser et personnaliser des méthodes de protection des endpoints en réseau.

Avec l'intégration d'Active Directory et de l'administration basée sur les rôles, chaque rôle d'utilisateur, selon les autorisations associées, peut créer, configurer ou supprimer des stratégies et des profils pour des domaines spécifiques.



Conseil

Plusieurs installations de pare-feu sur le même endpoint peuvent produire des résultats inattendus. Envisagez de désinstaller les autres applications de pare-feu logicielles sur les agents OfficeScan avant de déployer et d'activer le pare-feu OfficeScan.

Les étapes suivantes sont nécessaires pour utiliser correctement le pare-feu OfficeScan :

1. Créez une stratégie. Une stratégie vous permet de sélectionner un niveau de sécurité qui bloque ou autorise le trafic sur les endpoints en réseau et active les fonctions du pare-feu.
2. Ajoutez des exceptions à la stratégie. Les exceptions permettent aux agents OfficeScan de dévier d'une stratégie. Grâce aux exceptions, vous pouvez spécifier des agents et autoriser ou bloquer certains types de trafic malgré le niveau de sécurité défini dans la stratégie. Par exemple, vous pouvez bloquer tout le trafic

pour un ensemble d'agents dans une stratégie, mais créer une exception qui autorise le trafic HTTP pour que les agents puissent accéder à un serveur Web.

3. Créez et attribuez des profils aux agents OfficeScan. Un profil de pare-feu, qui comprend un ensemble d'attributs d'agents, est associé à une stratégie. Une fois qu'un agent correspond aux attributs spécifiés dans le profil, la stratégie associée est déclenchée.

Stratégies de pare-feu

Les stratégies de pare-feu vous permettent de bloquer ou d'autoriser certains types de trafic réseau non spécifiés dans une exception de stratégie. Une stratégie définit également les fonctions de pare-feu qui sont activées ou désactivées. Attribuez une stratégie à un ou plusieurs profils de pare-feu.

OfficeScan est fourni avec un ensemble de stratégies par défaut, que vous pouvez modifier ou supprimer.

Avec l'intégration d'Active Directory et de l'administration basée sur les rôles, chaque rôle d'utilisateur, selon les autorisations associées, peut créer, configurer ou supprimer des stratégies pour des domaines spécifiques.

Le tableau suivant répertorie les stratégies de pare-feu par défaut.

TABLEAU 12-1. Stratégies de pare-feu par défaut

NOM DE LA STRATÉGIE	NIVEAU DE SÉCURITÉ	PARAMÈTRES DES AGENTS	EXCEPTIONS	UTILISATION RECOMMANDÉE
Tous les accès	Faible	Activer le pare-feu	Aucune	À utiliser pour permettre aux agents un accès illimité au réseau
Ports de communication pour Trend Micro Control Manager	Faible	Activer le pare-feu	Autoriser tout le trafic TCP/UDP entrant/sortant via les ports 80 et 10319	À utiliser lorsque les agents ont une installation d'agent MCP

NOM DE LA STRATÉGIE	NIVEAU DE SÉCURITÉ	PARAMÈTRES DES AGENTS	EXCEPTIONS	UTILISATION RECOMMANDÉE
Console ScanMail for Microsoft Exchange	Faible	Activer le pare-feu	Autoriser tout le trafic TCP entrant/ sortant via le port 16372	À utiliser lorsque les agents veulent accéder à la console ScanMail
Console InterScan Messaging Security Suite (IMSS)	Faible	Activer le pare-feu	Autoriser tout le trafic TCP entrant/ sortant via le port 80	À utiliser lorsque les agents veulent accéder à la console IMSS

Créez également de nouvelles stratégies si vous avez des besoins non couverts par les stratégies par défaut.

Toutes les stratégies par défaut et créées par l'utilisateur s'affichent dans la liste des stratégies du pare-feu sur la console Web.

Configuration de la liste des stratégies du pare-feu

Procédure

1. Accédez à **Agents** > **Pare-feu** > **Stratégies**.
2. Pour ajouter une nouvelle stratégie, cliquez sur **Ajouter**.

   Si la nouvelle stratégie que vous souhaitez créer possède des paramètres similaires à ceux d'une stratégie existante, sélectionnez cette dernière et cliquez sur **Copier**. Pour modifier une stratégie existante, cliquez sur son nom.

   Un écran de configuration de stratégie s'affiche. Voir la *Ajout ou modification d'une stratégie de pare-feu à la page 12-11* pour plus d'informations.
3. Pour supprimer une stratégie existante, cochez la case en regard de la stratégie, puis cliquez sur **Supprimer**.
4. Pour modifier le modèle d'exception du pare-feu, cliquez sur **Modifier le modèle d'exception**.

Voir la *Modification du modèle d'exception du pare-feu à la page 12-14* pour plus d'informations.

L'éditeur de modèle d'exception apparaît.

Ajout ou modification d'une stratégie de pare-feu

Configurez ce qui suit pour chaque stratégie :

- **Niveau de sécurité** : Paramètre général qui bloque ou autorise tout le trafic entrant et/ou sortant sur le endpoint de l'agent OfficeScan.
- **Fonctionnalités du pare-feu** : Déterminez s'il convient d'activer ou de désactiver le pare-feu OfficeScan, le Système de détection d'intrusion (IDS) et le message de notification de violation de pare-feu. Voir *Système de détection d'intrusion à la page 12-4* pour obtenir des informations complémentaires sur SDI.
- **Liste Certified Safe Software** : spécifiez si vous souhaitez autoriser les applications certifiées comme sécurisées à se connecter au réseau. Voir *Liste Certified Safe Software à la page 12-3* pour obtenir des informations complémentaires sur la Liste Certified Safe Software.
- **Liste des exceptions de stratégie** : Liste d'exceptions configurables qui permet de bloquer ou d'accepter différents types de trafic réseau.

Ajout d'une stratégie de pare-feu

Procédure

1. Accédez à **Agents** > **Pare-feu** > **Stratégies**.
2. Pour ajouter une nouvelle stratégie, cliquez sur **Ajouter**.

   Si vous souhaitez créer une stratégie possédant des paramètres semblables à ceux d'une stratégie existante, sélectionnez cette dernière et cliquez sur **Copier**.
3. Entrez un nom pour la stratégie.
4. Sélectionnez un niveau de sécurité.

Le niveau de sécurité sélectionné ne s'applique pas au trafic répondant aux critères de l'exception de stratégie du pare-feu.

5. Sélectionnez les fonctions du pare-feu à utiliser pour la stratégie.

   - Le message de notification de violation du pare-feu s'affiche lorsque le pare-feu bloque un paquet sortant. Pour modifier le message, reportez-vous à *Modification du contenu du message de notification de pare-feu à la page 12-30*.

   - L'activation de toutes les fonctionnalités du pare-feu confère aux utilisateurs de l'agent OfficeScan les privilèges d'activation/de désactivation des fonctions et de modification des paramètres du pare-feu dans la console de l'agent OfficeScan.



AVERTISSEMENT!

Vous ne pouvez pas utiliser la console Web OfficeScan pour écraser les paramètres de la console de l'agent OfficeScan configurés par l'utilisateur.

   - Si vous n'activez pas ces fonctionnalités, les paramètres du pare-feu que vous configurez à partir de la console Web OfficeScan s'affichent sous **Liste des cartes réseau** sur la console de l'agent OfficeScan.

   - Les informations affichées sous **Paramètres**, sous l'onglet **Pare-feu** de la console de l'agent OfficeScan, reflètent toujours les paramètres configurés à partir de la console de l'agent OfficeScan et non de la console Web du serveur.

6. Activez la liste Certified Safe Software locale ou globale.



Remarque

Vérifiez que le service de prévention des modifications non autorisées et Certified Safe Software Services ont été activés avant d'activer ce service.

7. Sous Exception, sélectionnez les exceptions de stratégie de pare-feu. Les exceptions de stratégie répertoriées sont basées sur le modèle d'exception de pare-feu. Voir *Modification du modèle d'exception du pare-feu à la page 12-14* pour obtenir des informations détaillées.

- Modifiez une exception de stratégie existante en cliquant sur son nom et en modifiant les paramètres dans la page qui s'affiche.



Remarque

L'exception de stratégie modifiée ne s'appliquera qu'à la stratégie créée ultérieurement. Si vous souhaitez que la modification d'exception de stratégie soit permanente, vous devez apporter la même modification à l'exception de stratégie dans le modèle d'exception de pare-feu.

- Cliquez sur **Ajouter** pour créer une nouvelle exception de stratégie. Spécifiez les paramètres dans la page qui s'affiche.



Remarque

L'exception de stratégie ne s'appliquera également qu'à la stratégie créée ultérieurement. Pour appliquer cette exception de stratégie à d'autres stratégies, vous devez d'abord l'ajouter à la liste des exceptions de stratégies dans le modèle d'exception du pare-feu.

8. Cliquez sur **Enregistrer**.

Modification d'une stratégie de pare-feu existante

Procédure

1. Accédez à **Agents** > **Pare-feu** > **Stratégies**.
2. Cliquez sur une stratégie.
3. Modifiez ce qui suit :
    - Nom de la stratégie
    - Niveau de sécurité
    - Fonctions du pare-feu à utiliser pour la stratégie
    - État de la liste Certified Safe Software Service
    - Exceptions de stratégie de pare-feu à inclure à la stratégie

- Modifiez une exception de stratégie existante (cliquez sur le nom de l'exception de stratégie et modifiez les paramètres dans la page qui s'affiche)
- Cliquez sur **Ajouter** pour créer une nouvelle exception de stratégie. Spécifiez les paramètres dans la page qui s'affiche.

4. Cliquez sur **Enregistrer** pour appliquer les modifications à la stratégie existante.

Modification du modèle d'exception du pare-feu

Le modèle d'exception du pare-feu contient des exceptions de stratégie que vous pouvez configurer de manière à autoriser ou à bloquer divers types de trafic réseau à partir des numéros de port et des adresses IP des endpoints des agents OfficeScan. Lorsque vous avez créé une exception de stratégie, modifiez les stratégies auxquelles elle s'applique.

Choisissez le type d'exception de stratégie que vous voulez utiliser. Deux types sont proposés :

- **Les exceptions restrictives**

  Elles bloquent uniquement les types spécifiés de trafic réseau et s'appliquent aux stratégies qui autorisent tout le trafic réseau. Un exemple d'utilisation d'une exception de stratégie restrictive est de bloquer les ports des agents OfficeScan vulnérables aux attaques, tels que les ports souvent utilisés par les chevaux de Troie.

- **Les exceptions permissives**

  Elles autorisent uniquement les types spécifiés de trafic réseau et s'appliquent aux stratégies qui bloquent tout le trafic réseau. Par exemple, lorsque vous souhaitez autoriser des agents OfficeScan à accéder uniquement au serveur OfficeScan et à un serveur Web. Pour cela, autorisez le trafic depuis le port sécurisé (utilisé pour communiquer avec le serveur OfficeScan) et le port que l'agent OfficeScan utilise pour la communication HTTP.

  Port d'écoute de l'agent OfficeScan : **Agents** > **Gestion des agents > État**. Le numéro de port se trouve sous **Informations de base**.

  Port d'écoute du serveur : **Administration** > **Paramètres** > **Connexion de l'agent**. Le numéro de port se trouve sous **Paramètres de connexion de l'agent**.

OfficeScan est fourni avec un ensemble d'exceptions de stratégie de pare-feu par défaut, que vous pouvez modifier ou supprimer.

Tableau 12-2. Exceptions de stratégie de pare-feu par défaut

Nom de l'exception	Action	Protocole	Port	Direction
DNS	Autoriser	TCP/UDP	53	Entrant et sortant
NetBIOS	Autoriser	TCP/UDP	137, 138, 139, 445	Entrant et sortant
HTTPS	Autoriser	TCP	443	Entrant et sortant
HTTP	Autoriser	TCP	80	Entrant et sortant
Telnet	Autoriser	TCP	23	Entrant et sortant
SMTP	Autoriser	TCP	25	Entrant et sortant
FTP	Autoriser	TCP	21	Entrant et sortant
POP3	Autoriser	TCP	110	Entrant et sortant
LDAP	Autoriser	TCP/UDP	389	Entrant et sortant



Remarque

Les exceptions par défaut s'appliquent à tous les agents. Si vous souhaitez qu'une exception par défaut s'applique à certains agents seulement, modifiez-la et indiquez les adresses IP de ces agents.

L'exception LDAP n'est pas disponible si vous effectuez une mise à niveau à partir d'une version précédente d'OfficeScan. Ajoutez cette exception manuellement si vous ne la voyez pas dans la liste d'exceptions.

Ajout d'une exception de stratégie de pare-feu

Procédure

1. Accédez à **Agents** > **Pare-feu** > **Stratégies**.
2. Cliquez sur **Modifier le modèle d'exception**.
3. Cliquez sur **Ajouter**.
4. Entrez un nom pour l'exception de stratégie.
5. Sélectionnez le type d'application. Vous pouvez sélectionner toutes les applications ou spécifier un chemin d'application ou des clés de registre.



Remarque

Vérifiez le nom et les chemins complets saisis. L'exception d'application ne prend pas en charge les caractères génériques.

6. Sélectionnez l'action qu'OfficeScan effectuera sur le trafic réseau (bloquer ou autoriser le trafic qui répond au critère d'exception) et le sens du trafic (trafic réseau entrant ou sortant sur le endpoint de l'agent OfficeScan).
7. Sélectionnez le type de protocole réseau : TCP, UDP, ICMP ou ICMPv6.
8. Spécifiez les ports du endpoint de l'agent OfficeScan sur lesquels vous souhaitez exécuter l'action.
9. Sélectionnez les adresses IP des endpoints des agents OfficeScan à inclure dans l'exception. Par exemple, si vous choisissez de refuser tout le trafic réseau (entrant et sortant) et que vous saisissez l'adresse IP d'un seul endpoint sur le réseau, les agents OfficeScan dont la stratégie contient cette exception ne pourront pas envoyer de données vers cette adresse IP ou en recevoir à partir de celle-ci.
   - **Toutes les adresses IP** : comprend toutes les adresses IP
   - **Adresse IP unique** : saisissez une adresse IPv4 ou IPv6, ou un nom d'hôte.
   - **Plage (pour IPv4 ou IPv6)** : Saisissez une plage d'adresses IPv4 ou IPv6.
   - **Plage (pour IPv6)** : Saisissez le préfixe et la longueur d'une adresse IPv6.

- **Masque de sous-réseau** : Saisissez une adresse IPv4 et son masque de sous-réseau.

10. Cliquez sur **Enregistrer**.

Modification d'une exception de stratégie de pare-feu

Procédure

1. Accédez à **Agents** > **Pare-feu** > **Stratégies**.
2. Cliquez sur **Modifier le modèle d'exception**.
3. Cliquez sur une exception de stratégie.
4. Modifiez ce qui suit :
    - Nom de l'exception de stratégie
    - Type, nom ou chemin de l'application
    - Action qu'OfficeScan effectuera sur le trafic réseau et direction du trafic
    - Le type de protocole réseau
    - Les numéros de port de l'exception de stratégie
    - Adresses IP des endpoints des agents OfficeScan
5. Cliquez sur **Enregistrer**.

Enregistrement des paramètres de la liste d'exceptions de stratégie

Procédure

1. Accédez à **Agents** > **Pare-feu** > **Stratégies**.
2. Cliquez sur **Modifier le modèle d'exception**.

3. Cliquez sur l'une des options d'enregistrement suivantes :

    - **Enregistrer les modifications du modèle** : enregistre le modèle d'exception avec les exceptions de stratégie et les paramètres actuels. Cette option n'applique le modèle d'exception qu'aux stratégies créées ultérieurement, pas aux stratégies existantes.

    - **Enregistrer et appliquer aux stratégies existantes** : enregistre le modèle d'exception avec les exceptions de stratégie et les paramètres actuels. Cette option applique le modèle aux stratégies existantes et futures.

Profils de pare-feu

Les profils de pare-feu offrent une certaine flexibilité en vous permettant de sélectionner les attributs dont doit disposer un seul agent ou un groupe d'agents avant d'appliquer une stratégie. Créez des rôles utilisateur qui peuvent créer, configurer ou supprimer des profils pour des domaines spécifiques.

Les utilisateurs se servant du compte administrateur intégré ou ceux disposant d'autorisations de gestion complètes peuvent également activer l'option **Écraser le niveau de sécurité/la liste des exceptions de l'agent** pour remplacer les paramètres du profil de l'agent OfficeScan par les paramètres du serveur.

Les profils incluent les options suivantes :

- **Stratégie associée** : Chaque profil utilise une stratégie unique

- **Attributs de l'agent** : les agents OfficeScan disposant d'un ou de plusieurs des attributs suivants appliquent la stratégie associée°:

    - **Adresse IP** : un agent OfficeScan disposant d'une adresse IP spécifique, d'une adresse IP comprise dans une plage d'adresses IP ou d'une adresse IP appartenant à un sous-réseau spécifié.

    - **Domaine** : un agent OfficeScan appartenant à un domaine OfficeScan déterminé.

    - **Endpoint** : un agent OfficeScan associé à un nom de endpoint spécifique.

    - **Plate-forme** : un agent OfficeScan exécutant une plate-forme spécifique.

- **Nom de connexion** : endpoints des agents OfficeScan auxquels les utilisateurs spécifiés se sont connectés.
- **Description de la carte d'interface réseau** : tout endpoint d'un agent OfficeScan associé à une description de carte d'interface réseau correspondante.
- **État de la connexion de l'agent** : si l'agent OfficeScan est en ligne ou hors ligne.



Remarque

L'agent OfficeScan est en ligne lorsqu'il peut se connecter au serveur OfficeScan ou à l'un des serveurs de référence, et hors ligne s'il ne peut se connecter à aucun serveur.

OfficeScan est fourni avec un profil par défaut nommé « Tous les profils des agents » utilisant la stratégie « Tous les accès ». Vous pouvez modifier ou supprimer ce profil par défaut. Vous pouvez aussi créer de nouveaux profils. Tous les profils de pare-feu par défaut et créés par l'utilisateur, y compris la stratégie associée à chaque profil et l'état du profil actuel, s'affichent sur la liste des profils du pare-feu sur la console Web. Gérez la liste des profils et déployez tous les profils sur les agents OfficeScan. Les agents OfficeScan enregistrent tous les profils du pare-feu sur le endpoint de l'agent.

Configuration de la liste des profils du pare-feu

Procédure

1. Accédez à **Agents** > **Pare-feu** > **Profils**.
2. Les utilisateurs se servant du compte administrateur intégré ou ceux disposant d'autorisations de gestion complètes ont la possibilité d'activer l'option **Écraser le niveau de sécurité/la liste des exceptions de l'agent** pour remplacer les paramètres du profil de l'agent OfficeScan par les paramètres du serveur.
3. Pour ajouter un nouveau profil, cliquez sur **Ajouter**. Pour modifier un profil existant, sélectionnez son nom.

   Un écran de configuration de profil s'affiche. Voir *Ajout et modification d'un profil du pare-feu à la page 12-21* pour plus d'informations.

4. Pour supprimer une stratégie existante, cochez la case en regard de la stratégie, puis cliquez sur **Supprimer**.

5. Pour modifier l'ordre des profils dans la liste, cochez la case en regard du profil à déplacer, puis cliquez sur **Monter** ou **Descendre**.

   OfficeScan applique les profils du pare-feu aux agents OfficeScan dans l'ordre dans lequel les profils apparaissent dans la liste. Par exemple, si un agent correspond au premier profil, OfficeScan applique à l'agent les actions configurées pour ce profil. Les autres profils également configurés pour cet agent sont ignorés par OfficeScan.



Conseil

Placez les stratégies les plus exclusives au sommet de la liste. Placez par exemple une stratégie que vous créez pour un agent unique au sommet de la liste, suivies des stratégies qui concernent une gamme d'agents, un domaine réseau, puis enfin celles qui concernent tous les agents.

6. Pour gérer les serveurs de référence, cliquez sur **Modifier la liste de serveurs de référence**. Les serveurs de référence sont des endpoints qui remplacent le serveur OfficeScan lors de l'application des profils de pare-feu. Un serveur de référence peut être n'importe quel endpoint se trouvant sur le réseau (voir *Serveurs de référence à la page 13-30* pour plus d'informations). OfficeScan suppose que les conditions suivantes sont remplies lorsque vous activez des serveurs de référence :

   - Les agents OfficeScan connectés à des serveurs de référence sont en ligne, même si les agents ne peuvent pas communiquer avec le serveur OfficeScan.

   - Les profils du pare-feu appliqués à des agents OfficeScan en ligne s'appliquent également aux agents OfficeScan connectés à des serveurs de référence.



Remarque

Seuls les utilisateurs du compte d'administrateur intégré ou ceux disposant d'autorisations de gestion complètes peuvent voir et configurer la liste des serveurs de référence.

7. Pour enregistrer les paramètres actuels et attribuer les profils aux agents OfficeScan :

a. Vous pouvez choisir l'option **Écraser le niveau de sécurité/la liste des exceptions de l'agent**. Cette option écrase tous les paramètres de pare-feu configurés par l'utilisateur.

b. Cliquez sur **Affecter un profil aux agents**. OfficeScan attribue à tous les agents OfficeScan l'ensemble des profils figurant dans la liste.

8. Pour vérifier que les profils ont été correctement attribués aux agents OfficeScan :

a. Accédez à **Agents** > **Gestion des agents**. Sélectionnez **Affichage Pare-feu** dans la liste déroulante d'affichage de l'arborescence des agents.

b. Vérifiez la présence d'une coche verte dans la colonne **Pare-feu** de l'arborescence des agents. Si la stratégie associée au profil autorise le système de détection d'intrusion, une coche verte s'affiche également dans la colonne **SDI**.

c. Vérifiez que l'agent applique la bonne stratégie de pare-feu. La stratégie apparaît dans la colonne **Stratégie de pare-feu** dans l'arborescence des agents.

Ajout et modification d'un profil du pare-feu

Les endpoints des agents OfficeScan peuvent exiger différents niveaux de protection. Les profils du pare-feu vous permettent de préciser les endpoints des agents auxquels s'applique une stratégie associée. Généralement, un profil par stratégie utilisée est nécessaire.

Ajout d'un profil de pare-feu

Procédure

1. Accédez à **Agents** > **Pare-feu** > **Profils**.
2. Cliquez sur **Ajouter**.
3. Cliquez sur **Activer ce profil** pour qu'OfficeScan puisse déployer ce profil sur les agents OfficeScan.

4. Saisissez un nom d'identification du profil, ainsi qu'une description facultative.

5. Sélectionnez une stratégie pour ce profil.

6. Spécifiez les endpoints des agents sur lesquels OfficeScan applique la stratégie. Sélectionnez les endpoints en fonction des critères suivants :

    - adresse IP

    - Domaine : cliquez sur ce bouton pour ouvrir l'arborescence des agents et y sélectionner des domaines.

    Remarque

    Seuls les utilisateurs disposants d'autorisations complètes sur les domaines peuvent sélectionner des domaines.

    - Nom de l'Endpoint : cliquez sur ce bouton pour ouvrir l'arborescence des agents et y sélectionner des endpoints d'agents OfficeScan.

    - Plate-forme

    - Nom de connexion

    - Description de la carte d'interface réseau : Saisissez une description complète ou partielle, sans caractères de substitution.

    Conseil

    Trend Micro recommande de saisir le fabricant de la carte d'interface réseau (NIC) car les descriptions NIC commencent en général par le nom du fabricant. Par exemple, si vous avez saisi « Intel », toutes les cartes d'interface réseau fabriquées par Intel rempliront les critères. Si vous avez saisi un modèle de carte d'interface réseau particulier, par exemple « Intel(R) Pro/100 », seules les descriptions NIC commençant par « Intel(R) Pro/100 » rempliront les critères.

    - État de la connexion de l'agent

7. Cliquez sur **Enregistrer**.

Modification d'un profil de pare-feu

Procédure

1. Accédez à **Agents** > **Pare-feu** > **Profils**.
2. Cliquez sur un profil.
3. Cliquez sur **Activer ce profil** pour qu'OfficeScan puisse déployer ce profil sur les agents OfficeScan. Modifiez ce qui suit :
    - Le nom et la description du profil
    - La stratégie attribuée au profil
    - Les endpoints des agents OfficeScan, basés sur les critères suivants :
        - adresse IP
        - Domaine : cliquez sur ce bouton pour ouvrir l'arborescence des agents et y sélectionner des domaines.
        - Nom de l'Endpoint : cliquez sur ce bouton pour ouvrir l'arborescence des agents et y sélectionner des endpoints d'agents.
        - Plate-forme
        - Nom de connexion
        - Description de la carte d'interface réseau : Saisissez une description complète ou partielle, sans caractères de substitution.



Conseil

Trend Micro recommande de saisir le fabricant de la carte d'interface réseau (NIC) car les descriptions NIC commencent en général par le nom du fabricant. Par exemple, si vous avez saisi « Intel », toutes les cartes d'interface réseau fabriquées par Intel rempliront les critères. Si vous avez saisi un modèle de carte d'interface réseau particulier, par exemple « Intel(R) Pro/100 », seules les descriptions NIC commençant par « Intel(R) Pro/100 » rempliront les critères.

        - État de la connexion de l'agent

4. Cliquez sur **Enregistrer**.

Privilèges du pare-feu

Autorisent les utilisateurs à configurer leurs propres paramètres de pare-feu. Tous les paramètres configurés par l'utilisateur ne peuvent pas être remplacés par des paramètres déployés à partir du serveur OfficeScan. Par exemple, si l'utilisateur désactive le système de détection d'intrusion (SDI) et si vous activez SDI sur le serveur OfficeScan, SDI reste désactivé sur le endpoint de l'agent OfficeScan.

Activez les paramètres suivant pour permettre aux utilisateurs de configurer le pare-feu :

- **Afficher les paramètres du pare-feu sur la console de l'agent OfficeScan**

  L'option **Pare-feu** affiche tous les paramètres du pare-feu sur l'agent OfficeScan.

- **Autoriser les utilisateurs à activer/désactiver le pare-feu, le système de détection d'intrusion et le message de notification de violation du pare-feu**

  Le pare-feu OfficeScan protège les agents et les serveurs du réseau grâce à une fonction « Stateful inspection », à un scan antivirus de réseau hautes performances et à l'élimination des virus de réseau. Si vous accordez aux utilisateurs le privilège d'activer ou de désactiver le pare-feu et ses fonctionnalités, avertissez-les de ne pas désactiver le pare-feu trop longtemps, afin d'éviter d'exposer le endpoint aux intrusions et aux attaques de pirates.

  Si vous n'accordez pas ces privilèges aux utilisateurs, les paramètres du pare-feu que vous configurez depuis la console Web du serveur OfficeScan s'affichent sous Liste des cartes réseau sur la console de l'agent OfficeScan.

- **Autoriser les agents à envoyer les journaux du pare-feu au serveur OfficeScan**

  Sélectionnez cette option pour analyser le trafic que le pare-feu OfficeScan bloque et autorise. Pour plus d'informations sur les journaux de pare-feu, voir *Journaux de pare-feu à la page 12-30*.

  Si vous sélectionnez cette option, configurez la programmation d'envoi de journaux dans **Agents** > **Paramètres de l'agent général**. Rendez-vous à la section

Paramètres du pare-feu. La programmation ne s'applique qu'aux agents disposant du privilège d'envoi des journaux de pare-feu. Pour des instructions, voir *Paramètres généraux du pare-feu à la page 12-26*.

Accord des privilèges de pare-feu

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Dans l'onglet **Privilèges**, accédez à la section **Privilèges du pare-feu**.
5. Sélectionnez les options suivantes :
   - *Afficher l'onglet Pare-feu sur la console de l'agent OfficeScan à la page 12-24*
   - *Autoriser les utilisateurs à activer/désactiver le pare-feu, le système de détection d'intrusion et le message de notification de violation du pare-feu à la page 12-24*
   - *Autoriser les agents OfficeScan à envoyer les journaux du pare-feu au serveur OfficeScan à la page 12-24*
6. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :
   - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet

pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Paramètres généraux du pare-feu

Les paramètres généraux du pare-feu peuvent être appliqués aux agents OfficeScan de diverses manières.

- Un paramètre particulier du pare-feu peut être appliqué à tous les agents gérés par le serveur.
- Il est possible qu'un paramètre ne s'applique à l'agent OfficeScan que selon certains privilèges du pare-feu. Par exemple, le journal de pare-feu envoyant une programmation ne s'applique qu'aux agents OfficeScan ayant le privilège d'envoyer des journaux au serveur.

Activez les paramètres généraux suivants selon vos besoins :

- **Envoyer des journaux de pare-feu au serveur**

  Vous pouvez accorder à certains agents OfficeScan le privilège d'envoyer des journaux de pare-feu au serveur OfficeScan. Configurez la programmation d'envoi de journaux dans cette section. Seuls les agents bénéficiant du privilège d'envoi de journaux de pare-feu peuvent utiliser cette programmation.

  Voir *Privilèges du pare-feu à la page 12-24* pour obtenir des informations relatives aux privilèges de pare-feu disponibles pour certains agents.

- **Mettre à jour le pilote du pare-feu OfficeScan uniquement après le redémarrage du système**

  Permettez à l'agent OfficeScan de mettre à jour le pilote du pare-feu commun uniquement après le redémarrage du endpoint de l'agent OfficeScan. Activez cette option pour éviter des anomalies potentielles sur le endpoint de l'agent (telles qu'une déconnexion temporaire du réseau) lorsque le pilote du pare-feu commun se met à jour pendant une mise à niveau de l'agent.



Remarque

Cette fonctionnalité n'est disponible que pour les agents mis à niveau depuis OfficeScan 8.0 SP1 et versions ultérieures.

- **Envoyer au serveur OfficeScan les informations du journal du pare-feu toutes les heures pour déterminer si une épidémie du pare-feu survient**

  Lorsque vous activez cette option, les agents OfficeScan communiquent une fois par heure au serveur OfficeScan le nombre d'entrées du journal de pare-feu. Pour plus d'informations sur les journaux de pare-feu, voir *Journaux de pare-feu à la page 12-30*.

  OfficeScan utilise le nombre d'entrée des journaux et les critères liés aux épidémies de violation du pare-feu pour déterminer si une épidémie du pare-feu survient. Lors d'une épidémie, OfficeScan envoie des notifications par courrier électronique aux administrateurs OfficeScan.

- Accédez à la section **Paramètres de Certified Safe Software Service** et activez Certified Safe Software Service selon vos besoins.

  Certified Safe Software Service interroge les centres de données Trend Micro pour vérifier la sécurité d'un programme détecté par le blocage du comportement des programmes malveillants, la surveillance des événements, le pare-feu ou les scans antivirus. Activez le service Certified Safe Software Service pour réduire la probabilité de détection de faux-positifs.



Remarque

Vérifiez que les agents OfficeScan disposent des paramètres proxy corrects (pour plus d'informations, voir *Paramètres proxy des agents OfficeScan à la page 14-51*) avant d'activer Certified Safe Software Service. Des paramètres proxy incorrects, de même qu'une connexion Internet intermittente, peuvent entraîner des retards ou un échec de réception d'une réponse des centres de données Trend Micro, et faire que des programmes apparaissent comme sans réponse.

De plus, les agents OfficeScan IPv6 purs ne peuvent pas interroger directement les centres de données Trend Micro. Un serveur proxy à double pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre aux agents OfficeScan de se connecter aux centres de données Trend Micro.

Configuration des paramètres généraux de pare-feu

Procédure

1. Accédez à **Agents** > **Paramètres généraux de l'agent**.
2. Allez aux sections suivantes et configurez les paramètres :

TABLEAU 12-3. Paramètres généraux du pare-feu

SECTION	PARAMÈTRES
Paramètres du pare-feu	• *Envoyer des journaux de pare-feu au serveur à la page 12-26* • *Mettre à jour le pilote du pare-feu OfficeScan uniquement après le redémarrage du système à la page 12-26*
Nombre d'entrées du journal du pare-feu	*Envoyer au serveur OfficeScan les informations du journal du pare-feu toutes les heures pour déterminer si une épidémie du pare-feu survient à la page 12-27*
Paramètres Certified Safe Software	*Activer Certified Safe Software Service pour la surveillance des comportements, le pare-feu et les scans antivirus à la page 12-27*

3. Cliquez sur **Enregistrer**.

Notifications de violation du pare-feu pour les utilisateurs des agents OfficeScan

OfficeScan peut afficher un message de notification sur les agents immédiatement après le blocage par le pare-feu OfficeScan de trafic sortant allant à l'encontre des stratégies de pare-feu. Accordez aux utilisateurs le privilège d'activer/désactiver le message de notification.



Remarque

Vous pouvez également activer la notification lorsque vous configurez une stratégie de pare-feu spécifique. Pour configurer une stratégie de pare-feu, voir *Ajout ou modification d'une stratégie de pare-feu à la page 12-11*.

Accorder aux utilisateurs le privilège d'activer/désactiver le message de notification

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Dans l'onglet **Privilèges**, accédez à la section **Privilèges du pare-feu**.
5. Sélectionnez **Autoriser les utilisateurs à activer/désactiver le pare-feu, le système de détection d'intrusion et le message de notification de violation du pare-feu**.
6. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :
   - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Modification du contenu du message de notification de pare-feu

Procédure

1. Accédez à **Administration** > **Notifications** > **Agent**.
2. Dans la liste déroulante **Type**, sélectionnez **Violations du pare-feu**.
3. Saisissez les messages par défaut dans la zone de texte prévue à cet effet.
4. Cliquez sur **Enregistrer**.

Journaux de pare-feu

Les journaux de pare-feu disponibles sur le serveur sont envoyés par les agents OfficeScan disposant du privilège d'envoyer des journaux de pare-feu. Accordez à certains agents ce privilège pour surveiller et analyser le trafic sur les endpoints situés derrière le pare-feu OfficeScan.

Pour plus d'informations sur les privilèges du pare-feu, voir *Privilèges du pare-feu à la page 12-24*.

Pour éviter que les journaux n'occupent trop d'espace sur votre disque dur, vous pouvez les supprimer manuellement ou configurer leur suppression programmée. Voir *Gestion du journal à la page 13-36* pour obtenir des informations complémentaires sur la gestion des journaux.

Affichage des journaux du pare-feu

Procédure

1. Accédez à **Journaux** > **Agents** > **Risques de sécurité** ou **Agents** > **Gestion des agents**.

2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.

3. Cliquez sur **Journaux** > **Journaux de pare-feu** ou sur **Afficher journaux** > **Journaux de pare-feu**.

4. Pour être certain de disposer des journaux les plus à jour, cliquez sur **Notifier les agents**. Patientez jusqu'à ce que les agents aient envoyé les journaux de pare-feu avant de passer à l'étape suivante.

5. Spécifiez les critères de journaux, puis cliquez sur **Afficher les journaux**.

6. Affichez les journaux. Les journaux contiennent les informations suivantes :

   - Date et heure de la détection de violation du pare-feu
   - Endpoint sur lequel la violation du pare-feu s'est produite
   - Domaine du endpoint sur lequel la violation du pare-feu s'est produite
   - Adresse IP de l'hôte distant
   - Adresse IP de l'hôte local
   - Protocole
   - Numéro de port
   - Direction : si le trafic entrant (Recevoir) ou sortant (Envoyer) a violé une stratégie du pare-feu
   - Processus : le programme exécutable ou le service s'exécutant sur le endpoint qui a entraîné la violation du pare-feu
   - Description : définit le risque de sécurité effectif (tel qu'un virus de réseau ou une attaque SDI) ou la violation de stratégie de pare-feu

7. Pour sauvegarder les journaux dans un fichier `CSV` (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Épidémies de violation du pare-feu

Définissez une épidémie de violations du pare-feu selon le nombre de violations de pare-feu et la période de détection.

OfficeScan est fourni avec un message de notification par défaut vous informant, ainsi que les autres administrateurs OfficeScan, d'une épidémie. Vous pouvez modifier le message de notification en fonction de vos besoins.



Remarque

OfficeScan peut vous envoyer des notifications d'épidémies du pare-feu par e-mail. Configurez les paramètres de messagerie pour permettre à OfficeScan d'envoyer des e-mails correctement. Pour obtenir des informations détaillées, voir *Paramètres de notification aux administrateurs à la page 13-33*.

Configuration des critères et notifications de l'épidémie de violation du pare-feu

Procédure

1. Accédez à **Administration** > **Notifications** > **Épidémie**.
2. Dans l'onglet **Critères** :
    a. Accédez à la section **Violations du pare-feu**.
    b. Sélectionnez **Contrôler les violations du pare-feu sur les agents OfficeScan**.
    c. Spécifiez le nombre de journaux SDI, de journaux de pare-feu et de journaux de virus de réseau.
    d. Spécifiez la période de détection.



Conseil

Trend Micro recommande d'accepter les valeurs par défaut dans cet écran.

OfficeScan envoie un message de notification lorsque le nombre de journaux est dépassé. Par exemple, si vous spécifiez 100 journaux SDI, 100 journaux de pare-feu et 100 journaux de virus de réseau, ainsi qu'une période de 3 heures, OfficeScan envoie la notification lorsque le serveur reçoit 301 journaux sur une période de 3 heures.

3. Dans l'onglet **Courrier électronique** :

a. Accédez à la section **Épidémies de violation du pare-feu**.

b. Sélectionnez **Activer la notification par courrier électronique**.

c. Indiquez les destinataires de l'e-mail.

d. Acceptez ou modifiez l'objet et le message par défaut de l'e-mail. Vous pouvez utiliser des variables de jeton afin de représenter les données dans les champs **Objet** et **Message**.

TABLEAU 12-4. Variables de jeton pour les notifications d'épidémie de violation de pare-feu

VARIABLE	DESCRIPTION
%A	Le nombre d'entrées défini pour ce type de journal a été dépassé
%C	Nombre de journaux de violation du pare-feu
%T	Période d'accumulation des journaux de violation du pare-feu

4. Cliquez sur **Enregistrer**.

Test du pare-feu OfficeScan

Pour garantir le bon fonctionnement du pare-feu OfficeScan, effectuez un test sur un agent OfficeScan ou un groupe d'agents OfficeScan.



AVERTISSEMENT!

Testez les paramètres du programme de l'agent OfficeScan dans un environnement sous contrôle uniquement. N'effectuez aucun test sur des endpoints connectés au réseau ou à Internet. Cette opération peut exposer les endpoints des agents OfficeScan aux virus, aux attaques pirates, et à d'autres risques.

Procédure

1. Créez et enregistrez une stratégie de test. Configurez les paramètres pour bloquer les types de trafic que vous souhaitez tester. Par exemple, pour empêcher l'agent OfficeScan d'accéder à Internet, procédez comme suit :

   a. Configurez le niveau de sécurité sur **Faible** (Autoriser tout le trafic entrant/sortant).

   b. Sélectionnez **Activer le pare-feu et Avertir les utilisateurs en cas de violation du pare-feu**.

   c. Créez une exception bloquant le trafic HTTP (ou HTTPS).

2. Créez et enregistrez un profil de test en sélectionnant les agents sur lesquels vous souhaitez tester les fonctions de pare-feu. Associez la stratégie de test au profil de test.

3. Cliquez sur **Affecter un profil aux agents**.

4. Vérifiez le déploiement.

   a. Cliquez sur **Agents** > **Gestion des agents**.

   b. Sélectionnez le domaine auquel l'agent appartient.

   c. Sélectionnez **Affichage Pare-feu** dans l'affichage de l'arborescence des agents.

   d. Vérifiez la présence d'une coche verte dans la colonne **Pare-feu** de l'arborescence des agents. Si vous avez activé le système de détection d'intrusion pour cet agent, vérifiez qu'une coche verte est également présente sous la colonne **SDI**.

e. Vérifiez que l'agent applique la bonne stratégie de pare-feu. La stratégie apparaît dans la colonne **Stratégie de pare-feu** dans l'arborescence des agents.

5. Testez le pare-feu sur le endpoint de l'agent en essayant d'envoyer ou de recevoir le type de trafic que vous avez configuré dans la stratégie.

6. Pour tester une stratégie configurée pour empêcher l'agent d'accéder à Internet, ouvrez un navigateur Web sur le endpoint de l'agent. Si vous avez configuré OfficeScan pour qu'il affiche un message de notification pour les violations de pare-feu, le message s'affiche sur le endpoint de l'agent lorsqu'une violation de trafic sortant se produit.

Partie III

Gestion du serveur et des agents OfficeScan



Chapitre 13

Gestion du serveur OfficeScan

Ce chapitre décrit la gestion et les configurations du serveur OfficeScan.

Les rubriques sont les suivantes :

Administration basée sur les rôles

Utilisez la fonction d'Administration basée sur les rôles afin d'accorder et de contrôler l'accès à la console Web OfficeScan. Si votre entreprise compte plusieurs administrateurs OfficeScan, vous pouvez utiliser cette fonction pour accorder des privilèges spécifiques de console Web aux administrateurs, et leur proposer uniquement les outils et autorisations nécessaires à la mise en œuvre de ces tâches spécifiques. Vous pouvez également contrôler l'accès à l'arborescence des agents en leur donnant un ou plusieurs domaines à gérer. De plus, vous pouvez permettre aux non-administrateurs d'avoir un accès en «affichage seulement» à la console Web.

Chaque utilisateur (administrateur ou non) a un rôle spécifique. Un rôle définit le niveau d'accès à la console Web. Les utilisateurs se connectent à la console Web en utilisant des comptes utilisateurs personnalisés ou des comptes Active Directory.

La Role-based administration (administration basée sur les rôles) implique l'exécution des tâches suivantes :

1. Définissez les rôles utilisateurs. Pour plus d'informations, voir *Rôles de l'utilisateur à la page 13-2*.

2. Configurez les comptes utilisateurs et affectez un rôle spécifique à chaque compte utilisateur. Pour plus d'informations, voir *Comptes utilisateurs à la page 13-13*.

Affichez les activités de la console Web pour tous les utilisateurs à partir des Journaux des événements du système. Les activités suivantes sont consignées :

- Connexion à la console
- Modification du mot de passe
- Déconnexion de la console
- Expiration de la session (l'utilisateur est automatiquement déconnecté)

Rôles utilisateurs

Le rôle utilisateur détermine les options de menu de la console Web auxquelles un utilisateur peut accéder. Pour chaque option de menu, une autorisation est attribuée au rôle.

Attribuez des autorisations aux éléments suivants :

- *Autorisations de l'option de menu à la page 13-3*
- *Types d'options de menu à la page 13-3*
- *Options de menu pour les serveurs et les agents à la page 13-4*
- *Options de menu pour les domaines gérés à la page 13-7*

Autorisations de l'option de menu

Les autorisations déterminent le niveau d'accès à chaque option de menu. L'autorisation pour une option de menu peut être :

- **Configurer** : autorise l'accès complet à l'option de menu. Les utilisateurs peuvent configurer tous les paramètres, effectuer toutes les tâches, et accéder aux données dans une option de menu.
- **Afficher** : permet uniquement aux utilisateurs d'accéder aux paramètres, tâches et données d'une option de menu.
- **Aucun accès** : masque l'option de menu.

Types d'options de menu

Il existe 2 types d'options de menu configurables pour les rôles utilisateurs OfficeScan.

TABLEAU 13-1. Types d'options de menu

TYPE	ÉTENDUE
Options de menu pour les serveurs/ agents	• Paramètres, tâches et données du serveur • Données, tâches et paramètres généraux des agents Pour obtenir la liste complète des options de menu disponibles, voir *Options de menu pour les serveurs et les agents à la page 13-4*.

TYPE	ÉTENDUE
Options de menu pour les domaines gérés	Paramètres, tâches et données détaillés des agents, disponibles en dehors de l'arborescence des agents Pour obtenir la liste complète des options de menu disponibles, voir *Options de menu pour les domaines gérés à la page 13-7*.

Options de menu pour les serveurs et les agents

Le tableau suivant propose une liste des options de menu disponibles pour les serveurs/ agents.



Remarque

Les options de menu s'affichent seulement après l'activation de leur module additionnel respectif. Par exemple, si le module de prévention contre la perte de données n'est pas activé, aucune des options du menu Prévention contre la perte de données n'est présente dans la liste. Tout module additionnel supplémentaire s'affiche sous l'option de menu Modules additionnels.

Seuls les utilisateurs auxquels a été affecté le rôle « Administrateur (intégré) » ont accès à l'option de menu Modules additionnels.« »

TABLEAU 13-2. Options du menu Agents

OPTION DE MENU DE NIVEAU SUPÉRIEUR	OPTION DE MENU
Agents	• Gestion des agents • Regroupement des agents • Paramètres généraux de l'agent • Emplacement de l'Endpoint • Vérification de la connexion • Prévention des épidémies

TABLEAU 13-3. Options du menu Journaux

OPTION DE MENU DE NIVEAU SUPÉRIEUR	OPTION DE MENU
Journaux	• Agents • Risques de sécurité • Mise à jour des composants • Mises à jour du serveur • Événements système • Maintenance des journaux

TABLEAU 13-4. Options du menu Mises à jour

OPTION DE MENU DE NIVEAU SUPÉRIEUR	OPTION DE MENU	OPTION DE SOUS-MENU
Mises à jour	Serveur	• Mise à jour programmée • Mise à jour manuelle • Source de mise à jour
	Agents	• Mise à jour automatique • Source de mise à jour
	Rétrograder	N/A

TABLEAU 13-5. Options du menu Administration

OPTION DE MENU DE NIVEAU SUPÉRIEUR	OPTION DE MENU	OPTION DE SOUS-MENU
Administration	Gestion des comptes	• Comptes utilisateurs • Rôles utilisateurs

Option de menu de niveau supérieur	Option de menu	Option de sous-menu
		Remarque Seuls les utilisateurs se servant du compte administrateur intégré ont accès aux options Comptes utilisateurs et Rôles utilisateurs.
	Smart Protection	• Sources Smart Protection • Serveur intégré • Smart Feedback
	Active Directory	• Intégration d'Active Directory • Synchronisation programmée
	Notifications	• Paramètres généraux • Épidémie • Agent
	Paramètres	• Paramètres proxy • Paramètres de connexion de l'agent • Agents inactifs • Gestionnaire de quarantaine • Licence du produit • Paramètres de Control Manager • Paramètres de la console Web • Sauvegarde de la base de données

Option de menu de niveau supérieur	Option de menu	Option de sous-menu
	Outils	• Outils administrateurs • Outils de l'agent

Options de menu pour les domaines gérés

Le tableau suivant propose une liste des options de menu disponibles pour les domaines gérés.

Tableau 13-6. Option de menu Tableau de bord

Option de menu principale	Option de menu
Tableau de bord **Remarque** Tout utilisateur peut accéder à cette page, quelles que soient les autorisations dont il dispose.	N/A

Tableau 13-7. Options du menu Évaluation

Option de menu de niveau supérieur	Option de menu	Option de sous-menu
Évaluation	Conformité de la sécurité	• Rapport manuel • Rapport programmé
	Endpoints non gérés	N/A

TABLEAU 13-8. Options du menu Agents

OPTION DE MENU DE NIVEAU SUPÉRIEUR	OPTION DE MENU	OPTION DE SOUS-MENU
Agents	Pare-feu	• Stratégies • Profils
	Installation de l'agent	• Basé sur navigateur • Distant

TABLEAU 13-9. Options du menu Journaux

OPTION DE MENU DE NIVEAU SUPÉRIEUR	OPTION DE MENU	OPTION DE SOUS-MENU
Journaux	Agents	• Vérification de la connexion • Restauration depuis la mise en quarantaine centrale • Restauration des spywares/ graywares

TABLEAU 13-10. Options du menu Mises à jour

OPTION DE MENU DE NIVEAU SUPÉRIEUR	OPTION DE MENU	OPTION DE SOUS-MENU
Mises à jour	Résumé	N/A
	Agents	Mise à jour manuelle

TABLEAU 13-11. Options du menu Administration

OPTION DE MENU DE NIVEAU SUPÉRIEUR	OPTION DE MENU	OPTION DE SOUS-MENU
Administration	Notifications	Administrateur

Rôles utilisateurs intégrés

OfficeScan est fourni avec un ensemble de rôles utilisateurs intégrés que vous ne pouvez ni modifier ni supprimer. Les rôles intégrés sont les suivants :

TABLEAU 13-12. Rôles utilisateurs intégrés

NOM DU RÔLE	DESCRIPTION
Administrateur	Déléguez ce rôle à d'autres administrateurs ou utilisateurs d'OfficeScan ayant une connaissance suffisante d'OfficeScan. Les utilisateurs disposant de ce rôle peuvent configurer toutes les options de menu. **Remarque** Seuls les utilisateurs auxquels a été affecté le rôle « Administrateur (intégré) » ont accès à l'option de menu Modules additionnels.« »
Invité	Déléguez ce rôle aux utilisateurs qui souhaitent afficher la console Web à des fins de référence. • Les utilisateurs ayant ce rôle n'ont pas accès aux options de menu suivantes : • Modules additionnels • **Administration** > **Gestion des comptes** > **Rôles utilisateurs** • **Administration** > **Gestion des comptes** > **Comptes utilisateurs** • Les utilisateurs ont un accès en affichage à toutes les autres options du menu.
Trend Power User (rôle de mise à niveau uniquement)	Ce rôle est disponible uniquement si vous effectuez une mise à niveau vers OfficeScan 10. Ce rôle hérite des autorisations du rôle « Power User » dans OfficeScan 10. Les utilisateurs disposant de ce rôle peuvent configurer tous les domaines de l'arborescence des agents mais n'ont pas accès aux nouvelles fonctionnalités de cette version.

Rôles personnalisés

Vous pouvez créer des rôles personnalisés si aucun des rôles intégrés ne répond à vos besoins.

Seuls les utilisateurs ayant le rôle d'administrateur intégré et ceux qui utilisent le compte racine créé au cours de l'installation d'OfficeScan peuvent créer des rôles utilisateurs personnalisés et attribuer ces rôles aux comptes utilisateurs.

Ajout d'un rôle personnalisé

Procédure

1. Accédez à **Administration** > **Gestion des comptes** > **Rôles utilisateurs**
2. Cliquez sur **Ajouter**. Si le rôle que vous souhaitez créer possède des paramètres semblables à ceux d'un rôle existant, sélectionnez ce dernier et cliquez sur **Copier**.

   Un nouvel écran s'affiche.
3. Saisissez un nom pour le rôle, ainsi qu'une description facultative.
4. Cliquez sur **Options de menu pour les serveurs/agents** et spécifiez l'autorisation correspondant à chaque option de menu disponible. Pour obtenir la liste des options de menu disponibles, voir *Options de menu pour les serveurs et les agents à la page 13-4*.
5. Cliquez sur **Options de menu pour les domaines géré** et spécifiez l'autorisation correspondant à chaque option de menu disponible. Pour obtenir la liste des options de menu disponibles, voir *Options de menu pour les domaines gérés à la page 13-7*.
6. Cliquez sur **Enregistrer**.

   Le nouveau rôle s'affiche dans la liste des rôles utilisateurs.

Modification d'un rôle personnalisé

Procédure

1. Accédez à **Administration** > **Gestion des comptes** > **Rôles utilisateurs**
2. Cliquez sur le nom du rôle.

   Un nouvel écran s'affiche.
3. Effectuez les modifications nécessaires sur les éléments suivants :
   - Description
   - Autorisations de rôle
     - **Options de menu pour les serveurs/agents**
     - **Options de menu pour les domaines gérés**
4. Cliquez sur **Enregistrer**.

Suppression d'un rôle personnalisé

Procédure

1. Accédez à **Administration** > **Gestion des comptes** > **Rôles utilisateurs**
2. Cochez la case qui se trouve à côté du rôle.
3. Cliquez sur **Supprimer**.



Remarque

Un rôle ne peut pas être supprimé s'il est attribué à au moins un compte utilisateur.

Importation ou exportation de rôles personnalisés

Procédure

1. Accédez à **Administration** > **Gestion des comptes** > **Rôles utilisateurs**
2. Pour exporter les rôles personnalisés vers un ficher `.dat` :
   a. Sélectionnez les rôles et cliquez sur **Exporter**.
   b. Enregistrez le fichier `.dat`. Si vous gérez un autre serveur OfficeScan, utilisez le fichier `.dat` pour importer des rôles personnalisés dans ce serveur.



Remarque

Seule l'exportation des rôles entres les serveurs disposant d'une version identique est possible.

3. Pour exporter des rôles personnalisés vers un ficher `.csv` :
   a. Sélectionnez les rôles et cliquez sur **Export des paramètres de rôle**.
   b. Enregistrez le fichier `.csv`. Utilisez ce fichier pour vérifier les informations et autorisations des rôles sélectionnés.
4. Si vous avez enregistré des rôles personnalisés à partir d'un serveur OfficeScan différent et si vous souhaitez les importer dans le serveur OfficeScan actuel, cliquez sur **Importer** et recherchez le fichier `.dat` contenant les rôles personnalisés.
   - Dans l'écran Rôles utilisateur, un rôle sera écrasé si vous importez un rôle du même nom.
   - Seule l'importation des rôles entres les serveurs disposant d'une version identique est possible.
   - Un rôle importé à partir d'un autre serveur OfficeScan :
     - conserve les autorisations correspondant aux options de menus pour les serveurs/agents et aux options de menu pour les domaines gérés.
     - applique les autorisations par défaut pour les options du menu Gestion de l'agent. Sur l'autre serveur, enregistrez les autorisations du rôle pour

les options du menu Gestion de l'agent, puis réattribuez-les au rôle importé.

Comptes utilisateurs

Configurez les comptes utilisateurs et attribuez un rôle particulier à chaque utilisateur. Le rôle de l'utilisateur détermine les options de menu de la console Web qu'un utilisateur peut afficher et configurer.

Au cours de l'installation du serveur OfficeScan, le programme d'installation crée automatiquement un compte intégré nommé «racine». Les utilisateurs qui se connectent en utilisant le compte racine peuvent accéder à toutes les options du menu. Vous ne pouvez pas supprimer le compte racine mais vous pouvez modifier les détails du compte, par exemple le mot de passe et le nom complet ou la description du compte. Si vous oubliez le mot de passe du compte racine, contactez le service d'assistance pour qu'il vous aide à réinitialiser le mot de passe.

Ajoutez des comptes personnalisés ou des comptes Active Directory. Tous les comptes utilisateurs s'affichent dans la liste des comptes utilisateurs de la console Web.

Affectez des autorisations de comptes d'utilisateurs pour afficher ou configurer, au niveau individuel, les paramètres, les tâches et les données des agents disponibles dans l'arborescence des agents. Pour obtenir la liste complète des options de menu disponibles dans l'arborescence des agents, voir *Options du menu Gestion de l'agent à la page 13-13*.

Les comptes utilisateurs d'OfficeScan peuvent être utilisés pour l'«authentification unique». Celle-ci permet aux utilisateurs d'accéder à la console Web d'OfficeScan depuis la console de Trend Micro Control Manager. Pour plus d'informations, consultez la procédure suivante.

Options du menu Gestion de l'agent

Le tableau suivant propose une liste des options disponibles du menu Gestion de l'agent.



Remarque

Les options de menu s'affichent seulement après l'activation de leur module additionnel respectif. Par exemple, si le module de prévention contre la perte de données n'est pas activé, aucune des options du menu Prévention contre la perte de données n'est présente dans la liste.

TABLEAU 13-13. Options du menu Gestion de l'agent

OPTION DE MENU PRINCIPALE	SOUS-MENUS
État	N/A
Tâches	• Scan immédiat • Désinstallation de l'agent • Restauration depuis la mise en quarantaine centrale • Restauration des spywares/graywares

OPTION DE MENU PRINCIPALE	SOUS-MENUS
Paramètres	• Paramètres de scan • Méthodes de scan • Paramètres de scan manuel • Paramètres de scan en temps réel • Paramètres de scan programmé • Paramètres de scan immédiat • Paramètres de réputation de sites Web • Paramètres de connexion suspecte • Paramètres de surveillance des comportements • Paramètres de contrôle des dispositifs • Paramètres DLP • Paramètres des agents de mise à jour • Privilèges et autres paramètres • Paramètres des services complémentaires • Liste des spywares/graywares approuvés • exporter des paramètres • importer des paramètres

OPTION DE MENU PRINCIPALE	SOUS-MENUS
Journaux	• Journaux de virus/programmes malveillants • Journaux de spywares/graywares • Journaux de pare-feu • Journaux de réputation de sites Web • Journaux des connexions suspectes • Journaux de surveillance des comportements • Journaux de contrôle des dispositifs • Journaux de prévention contre la perte de données • Supprimer des journaux
Gestion de l'arborescence des agents	• Ajouter domaine • Renommer domaine • Déplacer un agent • Supprimer un domaine/agent
Exporter	Aucune

Ajout d'un compte personnalisé

Procédure

1. Accédez à **Administration** > **Gestion des comptes** > **Comptes utilisateurs**

2. Cliquez sur **Ajouter**.

   L'écran **Étape 1 Informations sur l'utilisateur** s'affiche.

3. Sélectionnez **Activer ce compte**.

4. Sélectionnez un rôle précédemment configuré dans la liste déroulante **Sélectionner un rôle**.

Pour plus d'informations sur la création de rôles utilisateurs, voir *Rôles personnalisés à la page 13-10*.

5. Saisissez le nom d'utilisateur, sa description et un mot de passe, puis confirmez ce mot de passe.

6. Entrez une adresse électronique pour le compte.



Remarque

OfficeScan envoie les notifications à cette adresse e-mail. Les notifications informent le destinataire des risques de sécurité détectés et des transmissions d'actifs numériques. Pour plus de détails sur les notifications, voir *Notifications sur les risques liés à la sécurité pour les administrateurs à la page 7-84*.

7. Cliquez sur **Suivant**.

   L'écran **Étape 2 Contrôle de domaine de l'agent** s'affiche.

8. Définissez l'étendue de l'arborescence des agents en sélectionnant le domaine racine, ou bien un ou plusieurs domaines de cette arborescence.

   Pour le moment, seuls les domaines ont été définis. Le niveau d'accès aux domaines sélectionnés sera défini à l'étape 10.

9. Cliquez sur **Suivant**.

   L'écran **Étape 3 Définir le menu de l'arborescence des agents** s'affiche.

10. Cliquez sur les commandes **Options de menu disponibles**, puis spécifiez l'autorisation correspondant à chaque option de menu disponible. Pour obtenir la liste des options de menu disponibles, voir *Options du menu Gestion de l'agent à la page 13-13*.

    L'étendue de l'arborescence des agents que vous avez configurée à l'étape 8 détermine le niveau d'autorisation d'accès aux options de menu et définit les cibles de l'autorisation. L'étendue de l'arborescence des agents peut être le domaine racine (tous les agents) ou des domaines spécifiques de cette arborescence.

Tableau 13-14. Options du menu Gestion de l'agent et étendue de l'arborescence des agents

Critères	Étendue de l'arborescence des agents	
	Domaine racine	Domaines spécifiques
Autorisation de l'option de menu	Configurer, Afficher, ou Aucun accès	Configurer, Afficher, ou Aucun accès
Cible	Domaine racine (tous les agents) ou domaines spécifiques Par exemple, vous pouvez accorder à un rôle l'autorisation de configurer l'option de menu « Tâches » dans l'arborescence des agents. Si la cible est le domaine racine, l'utilisateur peut exécuter les tâches pour tous les agents. Si les cibles sont les domaines A et B, les tâches ne peuvent être exécutées que pour les agents des domaines A et B.	Uniquement les domaines sélectionnés. Par exemple, vous pouvez accorder à un rôle l'autorisation de configurer l'option de menu « Paramètres » dans l'arborescence des agents. Cela signifie que l'utilisateur peut déployer les paramètres, mais uniquement pour les agents des domaines sélectionnés.
	L'arborescence des agents ne s'affichera que si l'autorisation pour l'option de menu « Gestion des agents » sous « Options de menu pour les serveurs/agents » est « Afficher ».	

- Si vous cochez la case sous **Configurer**, la case qui se trouve sous **Afficher** est cochée automatiquement.
- Si vous ne cochez aucune case, l'autorisation est « Aucun accès ».
- Si vous configurez des autorisations pour un domaine spécifique, vous pouvez copier ces autorisations vers d'autres domaines en cliquant sur **Copier les paramètres du domaine sélectionné vers d'autres domaines**.

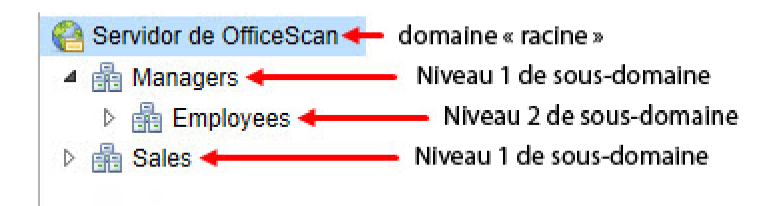
11. Cliquez sur **Terminer**.

12. Envoyez les détails du compte à l'utilisateur.

Définition des autorisations sur les domaines

Lors de la définition des autorisations sur les domaines, OfficeScan applique automatiquement les autorisations du domaine parent à tous les sous-domaines qu'il gère. Un sous-domaine ne peut pas disposer d'autorisations inférieures à celles octroyées à son domaine parent. Par exemple, si l'administrateur système dispose de l'autorisation d'afficher et de configurer tous les agents gérés par OfficeScan (le domaine « Serveur OfficeScan »), les autorisations des sous-domaines doivent permettre à l'administrateur système d'accéder à ces fonctionnalités de configuration. La suppression d'une autorisation sur un sous-domaine signifie que l'administrateur système ne dispose pas d'autorisations complètes de configuration sur tous les agents.

Pour la procédure ci-dessous, l'arborescence du domaine est la suivante :



Par exemple, pour octroyer au compte utilisateur « Chris » l'autorisation d'afficher et de configurer certaines options de menu pour le sous-domaine « Employés », mais lui permettre uniquement d'afficher les fichiers journaux du domaine parent « Responsables », procédez comme suit.

Tableau 13-15. Autorisations du compte utilisateur « Chris »

Domaine	Autorisations souhaitées
Serveur OfficeScan	Aucune autorisation spéciale
Responsables	Afficher les **Journaux**
Employés	Afficher et configurer les **Tâches** Afficher et configurer les **Journaux** Afficher les **Paramètres**
Service commercial	Aucune autorisation spéciale

Procédure

1. Accédez à l'écran **Comptes utilisateurs : Étape 3 Définir le menu de l'arborescence des agents**.

2. Cliquez sur le domaine « Serveur OfficeScan ».

3. Décochez toutes les cases **Afficher** et **Configurer**.



Remarque

Le domaine « Serveur OfficeScan » n'est configurable que si vous avez sélectionné tous ses sous-domaines sur l'écran **Comptes utilisateurs : Étape 2 Contrôle de domaine de l'agent**.

4. Cliquez sur le domaine « Service commercial ».

5. Décochez toutes les cases **Afficher** et **Configurer**.



Remarque

Le domaine « Service commercial » s'affiche uniquement s'il a été sélectionné sur l'écran **Comptes utilisateurs : Étape 2 Contrôle de domaine de l'agent**.

6. Cliquez sur le domaine « Responsables ».

7. Sélectionnez « Afficher les journaux » et décochez toutes les autres cases **Afficher** et **Configurer**.

8. Cliquez sur le domaine « Employés ».

9. Sélectionnez les options de menu suivantes pour Chris :

   - **Tâches** : Afficher et configurer
   - **Journaux** : Afficher et configurer
   - **Paramètres** : Afficher

   Chris peut désormais afficher et configurer les options de menu sélectionnées pour le domaine « Employés », mais peut uniquement afficher les **Journaux** du domaine « Responsables ».

Si Chris dispose des autorisations nécessaires pour afficher et configurer le domaine « Responsables », OfficeScan lui octroie automatiquement les mêmes autorisations sur le sous-domaine « Employés ». Cela se produit car le domaine « Responsables » gère tous ses sous-domaines.

Modification d'un compte personnalisé

Procédure

1. Accédez à **Administration** > **Gestion des comptes** > **Comptes utilisateurs**
2. Cliquez sur le compte utilisateur.
3. Activez ou désactivez le compte en cliquant sur la case à cocher fournie.
4. Modifiez ce qui suit :
   - Rôle
   - Description
   - Mot de passe
   - Adresse électronique
5. Cliquez sur **Suivant**.
6. Définissez l'étendue de l'arborescence des agents.
7. Cliquez sur **Suivant**.
8. Cliquez sur les commandes **Options de menu disponibles**, puis spécifiez l'autorisation correspondant à chaque option de menu disponible.

   Pour obtenir la liste des options de menu disponibles, voir *Options du menu Gestion de l'agent à la page 13-13*.
9. Cliquez sur **Terminer**.
10. Envoyez les nouveaux détails du compte à l'utilisateur.

Ajout de comptes ou de groupes Active Directory

Procédure

1. Accédez à **Administration** > **Gestion des comptes** > **Comptes utilisateurs**
2. Cliquez sur **Ajouter**.

   L'écran **Étape 1 Informations sur l'utilisateur** s'affiche.
3. Sélectionnez **Activer ce compte**.
4. Sélectionnez un rôle précédemment configuré dans la liste déroulante **Sélectionner un rôle**.

   Pour plus d'informations sur la création de rôles utilisateurs, voir *Rôles personnalisés à la page 13-10*.
5. Sélectionnez **Utilisateur ou groupe Active Directory**.
6. Recherchez un compte (nom d'utilisateur ou groupe) en indiquant le nom d'utilisateur et le domaine auquel il appartient.

   Remarque

   Utilisez le caractère (*) pour rechercher plusieurs comptes. Si vous n'utilisez pas le caractère générique, indiquez le nom complet du compte. Si les noms de compte sont incomplets ou si le groupe par défaut « Utilisateurs du domaine » est utilisé, OfficeScan ne renvoie aucun résultat.
7. Quand OfficeScan trouve un compte valide, il affiche son nom sous **Utilisateurs et groupes**. Cliquez sur l'icône de transfert (>) pour déplacer le compte sous **Utilisateurs et groupes sélectionnés**.

   Si vous indiquez un groupe Active Directory, tous les membres appartenant à un groupe ont le même rôle. Si un compte particulier appartient à deux groupes au moins et si le rôle des deux groupes est différent :

   - Les autorisations des deux rôles sont fusionnées. Si un utilisateur configure un paramètre particulier et s'il existe un conflit entre des autorisations pour ce paramètre, l'autorisation la plus élevée s'applique.

- Tous les rôles d'utilisateurs s'affichent dans les journaux d'événements du système. Par exemple, « l'utilisateur John Doe s'est connecté avec les rôles suivants : Administrateur, Power User».

8. Cliquez sur **Suivant**.

   L'écran **Étape 2 Contrôle de domaine de l'agent** s'affiche.

9. Définissez l'étendue de l'arborescence des agents.

10. Cliquez sur **Suivant**.

    L'écran **Étape 3 Définir le menu de l'arborescence des agents** s'affiche.

11. Cliquez sur les commandes **Options de menu disponibles**, puis spécifiez l'autorisation correspondant à chaque option de menu disponible.

    Pour obtenir la liste des options de menu disponibles, voir *Options du menu Gestion de l'agent à la page 13-13*.

12. Cliquez sur **Terminer**.

13. Demandez à l'utilisateur de se connecter à la console Web avec son compte de domaine et son mot de passe.

Trend Micro Control Manager

Trend Micro Control Manager™™ est une console d'administration centralisée qui gère les produits et services Trend Micro au niveau de la passerelle, du serveur de messagerie, du serveur de fichiers et des postes de travail des entreprises. La console d'administration à interface Web de Control Manager fournit un point de surveillance unique pour les produits et services gérés via le réseau.

Control Manager permet aux administrateurs système de surveiller et de notifier les activités telles que les infections, les violations de sécurité ou les points d'entrée de virus. Les administrateurs système peuvent télécharger et déployer des composants dans le réseau, contribuant ainsi à garantir une protection cohérente et à jour. Control Manager autorise les mises à jour à la fois manuelles et programmées, de même que la

configuration et la gestion des produits, en groupe ou séparément, afin d'obtenir une flexibilité accrue.

Intégration de Control Manager dans cette version d'OfficeScan

Cette version d'OfficeScan inclut les fonctionnalités suivantes pour administrer des serveurs OfficeScan à partir de Control Manager :

- Créez, gérez et déployez des stratégies pour l'antivirus, la prévention contre la perte de données ainsi que le contrôle des dispositifs OfficeScan et attribuez directement des privilèges aux agents OfficeScan à partir de la console Control Manager.

  Le tableau suivant énumère les configurations de stratégie disponibles sur Control Manager 6.0.

Tableau 13-16. Types de gestion de stratégie OfficeScan sur Control Manager

Type de stratégie	Fonctions
Antivirus et paramètres des agents OfficeScan	• Paramètres des services complémentaires • Paramètres de surveillance des comportements • Paramètres de contrôle des dispositifs • Paramètres de scan manuel • Privilèges et autres paramètres • Paramètres de scan en temps réel • Liste des spywares/graywares approuvés • Méthodes de scan • Paramètres de scan immédiat • Paramètres de scan programmé • Paramètres de connexion suspecte • Paramètres des agents de mise à jour • Paramètres de réputation de sites Web
Protection des données	Paramètres de la stratégie de prévention contre la perte de données **Remarque** Gérez les autorisations du contrôle des dispositifs pour la protection des données dans les stratégies des agents OfficeScan.

- Répliquez les paramètres suivants de la réputation de sites Web d'un serveur OfficeScan vers un autre à partir de la console Control Manager :

- *Types d'identificateurs de données à la page 10-6*
- *Modèles de prévention contre la perte de données à la page 10-21*



Remarque

Si ces paramètres sont répliqués vers des serveurs OfficeScan sur lesquels la licence de protection des données n'a pas été activée, ils ne sont pris en compte que lorsque la licence est activée.

Versions de Control Manager prises en charge

Cette version d'OfficeScan prend en charge les versions suivantes de Control Manager.

Tableau 13-17. Versions de Control Manager prises en charge

Serveur OfficeScan	Version de Control Manager		
	6.0 SP1	6.0	5.5 SP1
Double pile	Oui	Oui	Oui
IPv4 pur	Oui	Oui	Oui
IPv6 pur	Oui	Oui	Non



Remarque

L'adressage IPv6 est pris en charge pour Control Manager à partir de la version 5.5 Service Pack 1.

Pour plus d'informations sur les adresses IP faisant l'objet des rapports envoyés par le serveur et les agents OfficeScan à Control Manager, voir *Écrans affichant les adresses IP à la page A-7*.

Appliquez les patchs les plus récents et les correctifs de type hot fix critiques pour que ces versions de Control Manager permettent à Control Manager de gérer OfficeScan. Pour obtenir les patchs et les correctifs de type hot fix les plus récents, contactez le service d'assistance ou consultez le Centre de mises à jour Trend Micro à l'adresse :

http://downloadcenter.trendmicro.com/index.php?regs=fr

Après avoir installé OfficeScan, enregistrez-le dans Control Manager, puis configurez les paramètres d'OfficeScan dans la console d'administration de Control Manager. Consultez la *documentation de Control Manager* pour obtenir davantage d'informations sur la gestion des serveurs OfficeScan.

Enregistrement d'OfficeScan sur Control Manager

Procédure

1. Accédez à **Administration** > **Paramètres** > **Control Manager**.

2. Spécifiez le nom d'affichage de l'entité, qui est le nom du serveur OfficeScan devant s'afficher dans Control Manager.

   Par défaut, le nom d'affichage de l'entité inclut le nom d'hôte de l'ordinateur serveur et le nom de ce produit (par exemple, Server01_OSCE).

   Remarque

   Dans Control Manager, les serveurs OfficeScan et les autres produits gérés par Control Manager sont appelés «entités».

3. Spécifiez le nom de domaine complet ou l'adresse IP du serveur Control Manager et le numéro de port à utiliser pour la connexion à ce serveur. Si vous le souhaitez, vous pouvez optimiser la sécurité de la connexion via HTTPS.

   - Pour un serveur OfficeScan double-pile, saisissez le nom de domaine complet ou l'adresse IP de Control Manager (IPv4 ou IPv6, si disponible).
   - Pour un serveur OfficeScan IPv4, saisissez le nom de domaine complet ou l'adresse IPv4 de Control Manager
   - Pour un serveur OfficeScan IPv6, saisissez le nom de domaine complet ou l'adresse IPv6 de Control Manager

   Remarque

   Seul Control Manager 5.5 SP1 et versions ultérieures prennent en charge IPv6.

4. Si le serveur Web IIS de Control Manager requiert une authentification, saisissez le nom d'utilisateur et le mot de passe.

5. Si vous devez utiliser un serveur proxy pour vous connecter au serveur Control Manager, spécifiez les paramètres proxy suivants :

   - Protocole de serveur proxy
   - Nom de domaine complet ou adresse IPv4/IPv6 et port du serveur
   - ID d'utilisateur et mot de passe d'authentification du serveur proxy

6. Déterminez si vous souhaitez utiliser une redirection de port de communication unilatérale et bilatérale, puis spécifiez les adresses IPv4/IPv6 ainsi que le port.

7. Pour vérifier si OfficeScan peut se connecter au serveur Control Manager avec les paramètres spécifiés, cliquez sur **Tester la connexion**.

   Cliquez sur **Enregistrement** si la connexion a été établie.

8. Si la version du serveur Control Manager est la version 6.0 SP1 ou ultérieure, vous êtes invités par un message qui s'affiche à l'utiliser en tant que source de mise à jour pour le serveur Smart Protection Server intégré à OfficeScan. Cliquez sur **OK** pour utiliser le serveur Control Manager en tant que source de mise à jour du serveur Smart Protection Server intégré ou sur **Annuler** pour continuer à utiliser la source de mise à jour actuelle (par défaut, il s'agit du serveur ActiveUpdate).

9. Après l'enregistrement, si vous modifiez l'un des paramètres sur cet écran, cliquez sur **Paramètres de mise à jour** une fois les paramètres modifiés pour en informer le serveur Control Manager.

10. Si vous ne souhaitez plus que le serveur Control Manager gère OfficeScan, cliquez sur **Annuler l'enregistrement**.

Vérification de l'état d'OfficeScan sur la console d'administration de Control Manager

---

Procédure

1. Ouvrez la console d'administration de Control Manager.

Pour ouvrir la console Control Manager, ouvrez un navigateur Web sur un endpoint quelconque du réseau et entrez l'adresse suivante :

```
https://<nom du serveur Control Manager>/Webapp/login.aspx
```

Dans laquelle `<nom du serveur Control Manager>` correspond à l'adresse IP ou au nom d'hôte du serveur Control Manager.

2. Dans le menu principal, cliquez sur **Répertoires** > **Produits**.

3. Vérifiez si l'icône du serveur d'OfficeScan s'affiche

Outil d'exportation des stratégies

L'outil d'exportation des stratégies de Trend Micro OfficeScan Server aide les administrateurs à exporter les paramètres des stratégies OfficeScan prises en charge par Control Manager 6.0 ou version ultérieure. Les administrateurs ont également besoin de l'outil d'importation Control Manager afin d'importer les stratégies. L'outil d'exportation des stratégies prend en charge OfficeScan 10.6, Service Pack 1 ou version ultérieure.

- Paramètres de scan en temps réel
- Paramètres de scan programmé
- Paramètres de scan manuel
- Paramètres de scan immédiat
- Paramètres des agents de mise à jour
- Paramètres de réputation de sites Web
- Méthode de scan
- Paramètres de surveillance des comportements
- Paramètres de contrôle des dispositifs
- Paramètres de prévention contre la perte de données
- Privilèges et autres paramètres
- Paramètres des services complémentaires
- Liste des spywares/graywares approuvés
- Paramètres de connexion suspecte

Utilisation de l'outil d'exportation des stratégies

Procédure

1. Sur le serveur OfficeScan, accédez à <*Dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\PolicyExportTool`.
2. Double-cliquez sur `PolicyExportTool.exe` pour démarrer l'outil d'exportation des stratégies.

   Un écran d'interface de ligne de commande s'ouvre et l'outil d'exportation des stratégies commence à exporter les paramètres. L'outil crée deux dossiers (`PolicyClient` et `PolicyDLP`) dans le dossier `PolicyExportTool` contenant les paramètres exportés.
3. Copiez les deux dossiers dans le dossier d'installation de Control Manager.
4. Exécutez l'outil d'importation des stratégies sur le serveur Control Manager.

   Pour plus d'informations sur l'outil d'importation des stratégies, consultez *le fichier Lisez-moi de l'outil d'importation des stratégies*.



Remarque

L'outil d'exportation des stratégies n'exporte pas les identificateurs de données ou les modèles DLP personnalisés. Pour les administrateurs qui doivent exporter les identificateurs de données et les modèles DLP personnalisés, effectuez une exportation manuelle depuis la console OfficeScan, puis importez manuellement le fichier à l'aide de la console Control Manager.

Serveurs de référence

L'une des méthodes employées par l'agent OfficeScan pour déterminer les stratégies ou profils à utiliser consiste à vérifier son état de connexion avec le serveur OfficeScan. Si un agent OfficeScan interne (ou un agent se trouvant au sein du réseau d'entreprise) ne peut pas se connecter au serveur, l'agent passe à l'état hors ligne. L'agent applique ensuite un profil ou une stratégie destinée aux agents externes. Les serveurs de référence résolvent ce problème.

Un agent OfficeScan perdant sa connexion avec le serveur OfficeScan essaiera de se connecter aux serveurs de référence. Si l'agent parvient à établir une connexion avec le serveur de référence, il applique le profil ou la stratégie destinée aux agents internes.

Les stratégies et profils gérés par les serveurs de référence incluent :

- Profils de pare-feu
- Stratégies de réputation de sites Web
- Stratégies de protection des données
- Stratégies de contrôle des dispositifs

Prenez en compte les éléments suivants :

- Configurez les ordinateurs disposant de capacités de serveur, par exemple des serveurs Web, SQL ou FTP, comme serveurs de référence. Vous pouvez définir au maximum 32 serveurs de référence.
- Les agents OfficeScan se connectent au premier serveur de référence de la liste de serveurs de référence. Si la connexion ne peut pas être établie, l'agent essaie de se connecter au serveur suivant de la liste.
- Les agents OfficeScan n'utilisent les serveurs de référence que pour déterminer les paramètres à utiliser relatifs à l'antivirus (surveillance des comportements, contrôle des dispositifs, profils du pare-feu et stratégie de réputation de sites Web) ou à la protection des données. Les serveurs de référence ne gèrent pas les agents ni ne déploient les mises à jour et les paramètres agents. C'est le serveur OfficeScan qui effectue ces tâches.
- Un agent OfficeScan ne peut pas envoyer de journaux à des serveurs de référence ni les utiliser en tant que sources de mise à jour.

Gestion de la liste de serveurs de référence

Procédure

1. Accédez à **Agents** > **Pare-feu** > **Profils** ou **Agents** > **Emplacement de l'Endpoint**.

2. En fonction de l'écran qui s'affiche, vous devez procéder de la façon suivante :

   - Si vous vous trouvez sur l'écran **Profils de pare-feu pour les agents**, cliquez sur **Modifier la liste de serveurs de référence**.

   - Si vous vous trouvez sur l'écran **Emplacement de l'Endpoint**, cliquez sur la **liste de serveurs de référence**.

3. Sélectionnez **Activer la liste de serveurs de référence**.

4. Pour ajouter un endpoint à la liste, cliquez sur **Ajouter**.

   a. Spécifiez l'adresse IPv4/IPv6 du endpoint, son nom ou son nom de domaine complet (FQDN), par exemple :

      - `computer.networkname`
      - `12.10.10.10`
      - `mycomputer.domain.com`

   b. Saisissez le numéro de port au moyen duquel les agents communiquent avec ce endpoint. Spécifiez un port de contact ouvert quelconque (tels que les ports 20, 23 ou 80) sur le serveur de référence.

      
      Remarque

      pour spécifier un autre numéro de port pour le même serveur de référence, répétez les étapes 2a et 2b. L'agent OfficeScan utilise le premier numéro de port de la liste puis, en cas d'échec de connexion, le numéro de port suivant.

   c. Cliquez sur **Enregistrer**.

5. Pour modifier les paramètres d'un endpoint de la liste, cliquez sur son nom. Modifiez le nom ou le port du endpoint, puis cliquez sur **Enregistrer**.

6. Pour supprimer un endpoint de la liste, sélectionnez son nom, puis cliquez sur **Supprimer**.

7. Pour permettre aux endpoints de fonctionner en tant que serveurs de référence, cliquez sur **Affecter à des agents**.

Paramètres de notification aux administrateurs

Configurez les paramètres de notification aux administrateurs pour permettre à OfficeScan d'envoyer des notifications par courrier électronique et déroutement SNMP. OfficeScan peut également envoyer les notifications via le journal des événements Windows NT mais aucun paramètre n'est configuré pour ce canal de notifications.

OfficeSan peut vous envoyer des notifications, ainsi qu'à d'autres administrateurs OfficeScan dans les cas suivants :

TABLEAU 13-18. Détections qui entraînent la notification d'un administrateur

DÉTECTIONS	CANAUX DE NOTIFICATION		
	COURRIER ÉLECTRONIQUE	DÉROUTEMENT SNMP	JOURNAUX DES ÉVÉNEMENTS WINDOWS NT
Virus et programmes malveillants	Oui	Oui	Oui
Spywares et graywares	Oui	Oui	Oui
Transmissions des actifs numériques	Oui	Oui	Oui
Rappels C&C	Oui	Oui	Oui
Épidémies de virus et de programmes malveillants	Oui	Oui	Oui
Épidémies de spywares et de graywares	Oui	Oui	Oui
Épidémies de violation du pare-feu	Oui	Non	Non
Épidémies de sessions de partage de dossiers	Oui	Non	Non

Configuration des paramètres généraux de notification

Procédure

1. Accédez à **Administration** > **Notifications** > **Paramètres généraux**.
2. Configuration des paramètres de notification par e-mail.
   a. Indiquez une adresse IPv4/IPv6 ou le nom d'un endpoint dans le champ **Serveur SMTP**.
   b. Entrez un numéro de port compris entre 1 et 65535.
   c. Indiquez un nom ou une adresse e-mail.

      Si vous voulez activer ESMTP dans la prochaine étape, spécifiez une adresse e-mail valide.
   d. Eventuellement, activez **ESMTP**.
   e. Spécifiez le nom d'utilisateur et le mot de passe correspondant à l'adresse électronique que vous avez indiquée dans le champ **De**.
   f. Choisissez une méthode pour authentifier l'agent auprès du serveur :
      - **Connexion** : la connexion est une ancienne version de l'agent utilisateur de messagerie électronique. Le serveur et l'agent utilisent tous les deux BASE64 pour authentifier le nom d'utilisateur et le mot de passe.
      - **Texte brut** : le texte brut est le plus simple à utiliser mais il est également moins sûr car le nom d'utilisateur et le mot de passe sont envoyés sous forme d'une seule chaîne et sont codés en BASE64 avant leur envoi sur Internet.
      - **CRAM-MD5**: CRAM-MD5 utilise la combination d'un mécanisme d'authentification par stimulation/réponse et d'un algorithme cryptographique Message Digest 5 pour échanger et authentifier les informations.
3. Configuration des paramètres de notification de déroutement SNMP.
   a. Indiquez une adresse IPv4/IPv6 ou le nom d'un endpoint dans le champ **Adresse IP du serveur**.

b. Entrez un numéro de communauté difficile à deviner.

4. Cliquez sur **Enregistrer**.

Journaux des événements du système

OfficeScan enregistre les événements liés au programme serveur, tels que les arrêts et les démarrages. Ces journaux permettent de vérifier si le serveur et les services OfficeScan fonctionnent correctement.

Pour éviter que les journaux n'occupent trop d'espace sur votre disque dur, vous pouvez les supprimer manuellement ou configurer leur suppression programmée. Voir *Gestion du journal à la page 13-36* pour obtenir des informations complémentaires sur la gestion des journaux.

Affichage des journaux d'évènements du système

Procédure

1. Accédez à **Journaux** > **Événements système**.

2. Sous **Événement**, vérifiez les journaux pour lesquels une action supplémentaire est requise. OfficeScan consigne les événements suivants :

Tableau 13-19. Journaux des événements du système

Type de journal	Événements
Service principal d'OfficeScan et serveur de base de données	• Service principal démarré • Service principal fermé correctement • Échec de fermeture du service principal

TYPE DE JOURNAL	ÉVÉNEMENTS
Prévention des épidémies	• Prévention des épidémies activée • Prévention des épidémies désactivée • Nombre de sessions de partage de dossiers au cours des dernières <nombre de minutes>
Sauvegarde de la base de données	• Sauvegarde de la base de données réussie • Sauvegarde de la base de données impossible
Accès à la console Web basé sur les rôles	• Connexion à la console • Modification du mot de passe • Déconnexion de la console • Expiration de la session (l'utilisateur est automatiquement déconnecté)
Authentification serveur	• L'agent OfficeScan a reçu des commandes non valides de la part du serveur • Certificat d'authentification non valide ou ayant expiré

3. Pour sauvegarder les journaux dans un fichier `CSV` (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Gestion du journal

OfficeScan met à votre disposition des journaux complets concernant la détection des risques encourus par la sécurité, les événements, ainsi que les mises à jour. Utilisez ces journaux pour évaluer les stratégies de protection de votre entreprise et pour identifier les agents OfficeScan présentant un risque élevé d'infection ou d'attaque. Ils vous permettent également de vérifier la connexion agent-serveur et de vous assurer de la réussite des mises à jour des composants.

OfficeScan utilise également un mécanisme de vérification horaire centralisée pour garantir la cohérence de l'heure entre le serveur OfficeScan et les agents. Cela évite les

incohérences entre les journaux provoquées par des différences de fuseau horaire, l'heure d'été et les décalages horaires, qui peuvent engendrer une confusion lors de l'analyse des journaux.



Remarque

OfficeScan effectue la vérification horaire pour tous les journaux excepté les journaux de mise à jour du serveur et les journaux d'événements du système.

Le serveur OfficeScan reçoit les journaux suivants par les agents OfficeScan :

- *Affichage des journaux de virus/programmes malveillants à la page 7-92*
- *Affichage des journaux de spywares/graywares à la page 7-101*
- *Affichage des journaux des connexions suspectes à la page 11-27*
- *Affichage des journaux de restauration de spywares/graywares à la page 7-105*
- *Affichage des journaux du pare-feu à la page 12-30*
- *Affichage de journaux de réputation de sites Web à la page 11-25*
- *Affichage des journaux de rappel C&C à la page 11-26*
- *Affichage des journaux de surveillance des comportements à la page 8-16*
- *Affichage des journaux de contrôle des dispositifs à la page 9-19*
- *Affichage des journaux de prévention contre la perte de données à la page 10-57*
- *Affichage des journaux de mise à jour des agents OfficeScan à la page 6-56*
- *Affichage des journaux de vérification de la connexion à la page 14-46*

Le serveur OfficeScan génère les journaux suivants :

- *Journaux de mise à jour du serveur OfficeScan à la page 6-30*
- *Journaux des événements du système à la page 13-35*

Les journaux suivants sont également disponibles sur le serveur OfficeScan ainsi que les agents OfficeScan :

- *Journaux des événements Windows à la page 16-25*
- *Journaux du serveur OfficeScan à la page 16-3*
- *Journaux des agents OfficeScan à la page 16-16*

Maintenance des journaux

Pour éviter que les journaux occupent trop d'espace sur le disque dur, supprimez-les manuellement ou configurez un calendrier de suppression des journaux dans la console Web.

Suppression des journaux sur la base d'une programmation

Procédure

1. Accédez à **Journaux** > **Maintenance des journaux**.
2. Sélectionnez **Activer la suppression programmée des journaux**.
3. Sélectionnez les types de journaux à supprimer. Tous les journaux générés par OfficeScan, à l'exception des journaux de débogage, peuvent être supprimés en fonction d'un planning. Pour les journaux de débogage, désactivez la journalisation de débogage pour interrompre la collecte des journaux.



Remarque

Pour les journaux de virus/programmes malveillants, vous pouvez supprimer les journaux générés à partir de certains types de scan et de Damage Cleanup Services. Pour les journaux de spywares/graywares, vous pouvez supprimer les journaux de certains types de scan. Pour plus d'informations concernant les types de scan, voir *Types de scan à la page 7-15*.

---

4. Spécifiez si les journaux doivent être supprimés pour tous les types de journaux sélectionnés ou uniquement pour les journaux antérieurs à un certain nombre de jours.
5. Spécifiez la fréquence et l'heure de suppression des journaux.

6. Cliquez sur **Enregistrer**.

Suppression manuelle des journaux

Procédure

1. Accédez à **Journaux** > **Agents** > **Risques de sécurité** ou **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Effectuez l'une des opérations suivantes :
   - Si vous accédez à l'écran **Journaux des risques de sécurité**, cliquez sur **Supprimer des journaux**.
   - Si vous accédez à l'écran **Gestion des agents**, cliquez sur **Journaux** > **Supprimer des journaux**.
4. Sélectionnez les types de journaux à supprimer. Seuls les journaux suivants peuvent être supprimés manuellement :
   - Journaux de virus/programmes malveillants
   - Journaux de spywares/graywares
   - Journaux de pare-feu
   - Journaux de réputation de sites Web
   - Journaux des connexions suspectes
   - Journaux de rappel C&C
   - Journaux de surveillance des comportements
   - Journaux de contrôle des dispositifs
   - Journaux de prévention contre la perte de données



Remarque

Pour les journaux de virus/programmes malveillants, vous pouvez supprimer les journaux générés à partir de certains types de scan et de Damage Cleanup Services. Pour les journaux de spywares/graywares, vous pouvez supprimer les journaux de certains types de scan. Pour plus d'informations concernant les types de scan, voir *Types de scan à la page 7-15*.

5. Spécifiez si les journaux doivent être supprimés pour tous les types de journaux sélectionnés ou uniquement pour les journaux antérieurs à un certain nombre de jours.

6. Cliquez sur **Supprimer**.

Licences

Affichez, activez et renouvelez les services de licence OfficeScan sur la console Web et activez/désactivez le pare-feu OfficeScan. La pare-feu OfficeScan fait partie du service antivirus, qui inclut également la prise en charge de la prévention des épidémies.



Remarque

Certaines fonctionnalités natives d'OfficeScan, telles que la protection des données et Virtual Desktop Support, possèdent leurs propres licences. Les licences pour ces fonctions sont activées et gérées à partir de Plug-in Manager. Pour plus d'informations sur les licences de ces fonctionnalités, consultez *Licence de protection des données à la page 3-4* et *Licence de Virtual Desktop Support à la page 14-79*.

Un serveur IPv6 OfficeScan ne peut pas se connecter au serveur d'enregistrement en ligne Trend Micro pour activer ou renouveler la licence. Un serveur proxy double pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre au serveur OfficeScan de se connecter au serveur d'enregistrement.

Affichage des informations sur la licence produit

Procédure

1. Accédez à **Administration** > **Paramètres** > **Licence du produit**.

2. Affichez le récapitulatif de l'état des licences, qui apparaît en haut de l'écran. Des messages de rappel concernant les licences s'affichent dans les cas suivants:

   TABLEAU 13-20. Rappels de licence

TYPE DE LICENSE	RAPPEL
Version complète	• Pendant la période de grâce du produit : La durée de la période de grâce varie selon les régions. Veuillez vérifier cette durée auprès de votre représentant Trend Micro. • Une fois la licence expirée et la période de grâce écoulée: pendant cette période, vous ne pourrez ni obtenir d'assistance technique ni effectuer de mises à jour des composants. Les moteurs de scan continueront à scanner les ordinateurs mais utiliseront des composants obsolètes. Ces composants obsolètes ne peuvent pas vous protéger entièrement contre les derniers risques de sécurité.
Version d'évaluation	Une fois la licence expirée: pendant cette période, OfficeScan désactive les mises à jour des composants, les scans, ainsi que toutes les fonctionnalités des agents OfficeScan.

3. Affichez les informations de licence. La section **Informations sur la licence** vous fournit les informations suivantes :

   - **Services** : Comprend tous les services de licence d'OfficeScan
   - **État** : affiche « Activé », « Non activé », « Expiré » ou « En période de grâce ». Si un service dispose de plusieurs licences dont au moins une licence toujours active, l'état « Activé » s'affiche.
   - **Version** : affiche la version « complète » ou d'« évaluation ». Si vous disposez à la fois de la version complète et de versions d'évaluation, la version qui s'affiche alors est la version « complète ».

- **Date d'expiration** : Si un service a plusieurs licences, la dernière date d'expiration s'affiche. Par exemple, si les dates d'expiration de la licence sont le 31/12/2007 et le 30/06/2008, la date qui s'affiche est le 30/06/2008.



Remarque

« N/A » correspond aux dates de version et d'expiration des services de licence n'ont pas été activés.

4. OfficeScan vous autorise à activer plusieurs licences pour un service de licence. Cliquez sur le nom du service pour afficher toutes les licences (à la fois actives et expirées) de ce service.

Activation ou renouvellement d'une licence

Procédure

1. Accédez à **Administration** > **Paramètres** > **Licence du produit**.
2. Cliquez sur le nom du service de licence.
3. Dans l'écran **Détails sur la licence du produit** qui s'ouvre, cliquez sur **Nouveau code d'activation**.
4. Dans l'écran qui s'affiche, saisissez le code d'activation puis cliquez sur **Enregistrer**.



Remarque

Enregistrez un service avant de l'activer. Pour plus d'informations sur la clé d'enregistrement et le code d'activation, contactez votre revendeur Trend Micro.

5. Lorsque vous revenez à l'écran **Détails sur la licence du produit**, cliquez sur **Informations sur la mise à jour** pour actualiser l'écran avec les détails de la nouvelle licence et l'état du service. Cet écran fournit également un lien vers le site Web de Trend Micro sur lequel vous trouverez des informations détaillées relatives à votre licence.

Sauvegarde de la base de données d'OfficeScan

La base de données du serveur OfficeScan contient tous les paramètres OfficeScan, y compris les paramètres de scan et les privilèges. En cas d'altération de la base de données du serveur, vous pouvez la restaurer si vous disposez d'une copie de sauvegarde. Créez une sauvegarde de la base de données manuellement ou configurez un programme de sauvegarde.

Lorsque vous sauvegardez la base de données, OfficeScan vous aide automatiquement à la défragmenter et répare éventuellement toute détérioration du fichier d'index.

Consultez les journaux d'événements du système pour déterminer l'état de la sauvegarde. Pour plus d'informations, voir *Journaux des événements du système à la page 13-35*.



Conseil

Trend Micro recommande de configurer un programme de sauvegarde automatique. Sauvegardez la base de données durant les heures creuses, lorsque le trafic sur le serveur est faible.



AVERTISSEMENT!

N'effectuez pas de sauvegarde avec tout autre outil ou logiciel. Configurez la sauvegarde de la base de données uniquement à partir de la console Web d'OfficeScan.

Sauvegarde de la base de données OfficeScan

Procédure

1. Accédez à **Administration** > **Paramètres** > **Sauvegarde de la base de données**.
2. Entrez l'emplacement où vous souhaitez enregistrer la base de données. Si le dossier n'existe pas encore, sélectionnez **Créer le dossier s'il n'est pas encore présent**. Précisez le lecteur et le chemin d'accès complet du répertoire, par exemple : `c:\OfficeScan\DatabaseBackup`.

Par défaut, OfficeScan copie la sauvegarde dans le répertoire suivant : <*Dossier d'installation du serveur*>`\DBBackup`



Remarque

OfficeScan permet de créer un sous-dossier sous le chemin de sauvegarde. Le nom de dossier indique l'heure de la sauvegarde et se présente dans le format suivant : AAAAMMJJ_HHMMSS. OfficeScan conserve les 7 dossiers de sauvegarde les plus récents et supprime le(s) dossier(s) antérieur(s).

3. Si le chemin de sauvegarde désigne un ordinateur distant (en utilisant un chemin UNC), saisissez un nom de compte adapté et le mot de passe correspondant. Vérifiez que le compte dispose des privilèges d'écriture sur l'ordinateur.

4. Pour configurer un programme de sauvegarde :

    a. Sélectionnez **Activer la sauvegarde programmée de la base de données**.

    b. Spécifiez la fréquence et l'heure de sauvegarde.

    c. Pour sauvegarder la base de données et enregistrer les modifications apportées, cliquez sur **Sauvegarder maintenant**. Pour enregistrer sans sauvegarder la base de données, cliquez sur **Enregistrer**.

Restauration des fichiers de sauvegarde de la base de données

Procédure

1. Arrêtez le service principal d'OfficeScan.

2. Remplacez les fichiers de la base de données dans le répertoire <*dossier d'installation du serveur*>`\PCCSRV\HTTPDB` par les fichiers de sauvegarde.

3. Redémarrez le service principal d'OfficeScan.

Outil de migration SQL Server

Les administrateurs peuvent utiliser l'outil de migration SQL Server pour faire migrer la base de données OfficeScan existante de sa structure CodeBase native vers une base de données SQL Server. L'outil de migration SQL Server prend en charge les migrations de bases de données suivantes :

- D'une base de données CodeBase OfficeScan vers une nouvelle base de données SQL Server Express
- D'une base de données CodeBase OfficeScan vers une base de données SQL Server existant déjà
- D'une base de données SQL OfficeScan (précédemment migrée) déplacée vers un autre emplacement

Utilisation de l'outil de migration SQL Server

L'outil de migration SQL Server migre la base de données CodeBase existante vers une base de données SQL à l'aide de SQL Server 2008 R2 SP2 Express.



Conseil

Une fois la migration de la base de données OfficeScan effectuée, vous pouvez déplacer la base de données SQL récemment migrée vers un autre serveur SQL. Exécutez à nouveau l'outil de migration SQL Server et sélectionnez **Passer à une base de données SQL OfficeScan existante** pour utiliser l'autre serveur SQL.



Important

Avant d'exécuter l'outil de migration SQL Server sur une plate-forme Windows Server 2008 ou ultérieure à l'aide d'informations d'authentification d'utilisateur de domaine Windows :

- Le **Contrôle d'accès des utilisateurs** doit être désactivé
- Le Service principal d'OfficeScan ne peut pas être exécuté à l'aide du compte d'utilisateur de domaine servant à la connexion au serveur SQL

Procédure

1. Sur l'ordinateur du serveur OfficeScan, accédez au répertoire <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\SQL`.

2. Double-cliquez sur le fichier `SQLTxfr.exe` pour exécuter l'outil.

   La console de l'**Outil de migration SQL Server** s'ouvre.

3. Sélectionnez le type de migration :

Option	Description
Installer une nouvelle instance SQL Server 2008 R2 SP2 Express et migrer la base de données OfficeScan	Installe automatiquement SQL Server 2008 R2 SP2 Express et migre la base de données OfficeScan existante vers une nouvelle base de données SQL **Remarque** OfficeScan affecte automatiquement le port 1433 au serveur SQL.
Migrer la base de données OfficeScan vers une instance SQL Server existante	Migre la base de données OfficeScan existante vers une nouvelle base de données SQL sur un serveur SQL existant
Passer à une base de données SQL OfficeScan existante	Modifie les paramètres de configuration d'OfficeScan afin de pointer vers une base de données SQL OfficeScan existante sur un serveur SQL existant

4. Spécifiez le **Nom du serveur** comme suit :

   - Pour de nouvelles installations SQL : <nom de l'hôte ou adresse IP du serveur SQL>\<nom de l'instance>
   - Pour des migrations de serveurs SQL : <nom de l'hôte ou adresse IP du serveur SQL>,<numéro_de_port>\<nom de l'instance>
   - Lors du basculement vers une base de données SQL OfficeScan existante : <nom de l'hôte ou adresse IP du serveur SQL>,<numéro_de_port>\<nom de l'instance>



Important

OfficeScan crée automatiquement une instance de la base de données OfficeScan lors de l'installation du serveur SQL. Lors de la migration vers un serveur ou une base de données SQL existant(e), saisissez le nom de l'instance existante d'OfficeScan sur le serveur SQL.

5. Fournissez les informations d'authentification de la base de données du serveur SQL.



Important

Lors de l'utilisation d'un **Compte Windows** pour la connexion au serveur :

- Pour un compte d'administrateur de domaine par défaut :
    - Format du **Nom d'utilisateur** : nom_du_domaine\administrateur
    - Le compte requiert les éléments suivants :
        - Groupes : « Groupe Administrateurs »
        - Rôles utilisateurs : « Ouvrir une session en tant que service » et « Ouvrir une session en tant que tâche »
        - Rôles de base de données : « dbcreator », « bulkadmin » et « db_owner »
- Pour un compte d'utilisateur de domaine :
    - Format du **Nom d'utilisateur** : nom_de_domaine\nom_d'utilisateur
    - Le compte requiert les éléments suivants :
        - Groupes : « Groupe Administrateurs » et « Admins du domaine »
        - Rôles utilisateurs : « Ouvrir une session en tant que service » et « Ouvrir une session en tant que tâche »
        - Rôles de base de données : « dbcreator », « bulkadmin » et « db_owner »

6. Pour les nouvelles installations de serveur SQL, saisissez un nouveau mot de passe, puis confirmez-le.



Remarque

Les mots de passe doivent répondre aux critères minimaux suivants :

a. Longueur minimale : 6 caractères

b. Ils doivent contenir au moins 3 des éléments suivants :

- Lettres majuscules : A - Z
- Lettres minuscules : a - z
- Chiffres : 0 - 9
- Caractères spéciaux : !@#$^*?_~-();.+:

7. Indiquez le **Nom de la base de données** OfficeScan sur le serveur SQL.

   Lors de la migration de la base de données CodeBase OfficeScan vers une nouvelle base de données SQL, OfficeScan crée automatiquement une base de données portant le nom indiqué.

8. Vous avez éventuellement la possibilité d'effectuer les tâches suivantes :

   - Cliquez sur **Tester la connexion** pour vérifier les informations d'authentification du serveur ou de la base de données SQL existant(e).
   - Cliquez sur **Alerte d'indisponibilité de la base de données SQL...** pour configurer les paramètres de notification de la base de données SQL. Pour obtenir des informations détaillées, consultez la section *Configuration de l'alerte d'indisponibilité de la base de données SQL à la page 13-48*.

9. Cliquez sur **Démarrer** pour appliquer les modifications de la configuration.

Configuration de l'alerte d'indisponibilité de la base de données SQL

OfficeScan envoie automatiquement cette alerte lorsque la base de données SQL devient indisponible.



AVERTISSEMENT!

OfficeScan arrête automatiquement tous les services lorsque la base de données devient indisponible. OfficeScan ne peut pas consigner dans des journaux d'informations relatives aux agents ou aux événements, effectuer de mises à jour ni configurer d'agents lorsque la base de données est indisponible.

Procédure

1. Sur l'ordinateur du serveur OfficeScan, accédez au répertoire <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\SQL`.
2. Double-cliquez sur le fichier `SQLTxfr.exe` pour exécuter l'outil.

   La console de l'**Outil de migration SQL Server** s'ouvre.
3. Cliquez sur **Alerte d'indisponibilité de la base de données SQL...**.

   L'écran **Alerte d'indisponibilité de l'instance SQL Server** s'ouvre.
4. Saisissez les adresses électroniques des destinataires de l'alerte.

   Séparez les entrées multiples par des points virgules (;).
5. Modifiez les champs **Objet** et **Message** si nécessaire.

   OfficeScan fournit les variables de jeton suivantes :

   TABLEAU 13-21. Jetons d'alerte d'indisponibilité de la base de données SQL

VARIABLE	DESCRIPTION
%x	Nom de l'instance SQL Server OfficeScan
%s	Nom du serveur OfficeScan affecté

6. Cliquez sur **OK**.

Paramètres de connexion entre le serveur et les agents OfficeScan

Pendant l'installation du serveur OfficeScan, le programme d'installation installe automatiquement un serveur Web (IIS ou serveur Web Apache) qui permet aux ordinateurs en réseau de se connecter au serveur OfficeScan. Configurez le serveur Web auquel les agents des endpoints en réseau se connectent.

Si vous modifiez les paramètres de serveur Web de façon externe (par exemple, à partir de la console d'administration IIS), répliquez les modifications dans OfficeScan. Si, par exemple, vous changez manuellement l'adresse IP du serveur pour les ordinateurs en réseau ou si vous lui attribuez une adresse IP dynamique, vous devez reconfigurer les paramètres du serveur OfficeScan.



AVERTISSEMENT!

La modification des paramètres de connexion peut entraîner une perte de connexion permanente entre le serveur et les agents. Vous devrez alors redéployer les agents OfficeScan.

Configuration des paramètres de connexion

Procédure

1. Accédez à **Administration** > **Paramètres** > **Connexion de l'agent**.
2. Saisissez le nom de domaine ou l'adresse IPv4/IPv6 et le numéro de port du serveur Web.

   Remarque

   Le numéro de port correspond au port sécurisé que le serveur OfficeScan utilise pour communiquer avec les agents OfficeScan.

3. Cliquez sur **Enregistrer**.

Mot de passe de la console Web

L'écran permettant de gérer le mot de passe de la console Web (ou le mot de passe du compte racine créé au cours de l'installation du serveur OfficeScan) n'est accessible que si l'ordinateur serveur ne dispose pas des ressources requises pour utiliser l'administration basée sur les rôles. Par exemple, si l'ordinateur serveur exécute Windows Server 2003 et si Authorization Manager Runtime n'est pas installé, l'écran est accessible. Si les ressources sont adéquates, cet écran ne s'affiche pas et le mot de passe peut être géré en modifiant le compte racine dans l'écran **Comptes utilisateurs**.

Si OfficeScan n'est pas enregistré sur Control Manager, contactez votre service d'assistance pour savoir comment accéder à la console Web.

Authentification des communications provenant du serveur

OfficeScan utilise le chiffrement à clé publique pour authentifier les communications du serveur OfficeScan vers les agents. Grâce à cette technologie, le serveur conserve une clé privée et déploie une clé publique sur tous les agents. Les agents utilisent la clé publique pour vérifier que les communications entrantes proviennent bien du serveur et sont valides. Les agents répondent au serveur si cette vérification réussit.



Remarque

OfficeScan n'authentifie pas les communications vers le serveur provenant des agents.

Les clés, privée et publique, sont associées à un certificat émis par Trend Micro. Pendant l'installation du serveur OfficeScan, le programme d'installation range le certificat dans le magasin de certificats de l'hôte. Utilisez le Gestionnaire de certificats d'authentification pour gérer les certificats et les clés de Trend Micro.

Lorsque vous décidez de l'utilisation d'une clé d'authentification unique sur l'ensemble des serveurs OfficeScan, tenez compte des éléments suivants :

- La mise en œuvre d'une clé de certificat unique est une pratique courante pour assurer un niveau de sécurité standard. Cette approche permet d'équilibrer le niveau

de sécurité de votre organisation et évite les coûts associés à la gestion de clés multiples.

- La mise en œuvre de plusieurs clés de certificat sur les différents serveurs OfficeScan fournit un niveau de sécurité maximal. Cette approche augmente la maintenance nécessaire lorsque les clés de certificat expirent et doivent être redistribuées sur les serveurs.



Important

Avant de réinstaller le serveur OfficeScan, n'oubliez pas de sauvegarder le certificat existant. Une fois la nouvelle installation terminée, importez le certificat sauvegardé pour assurer la continuité de l'authentification de la communication entre le serveur OfficeScan et les agents OfficeScan. Si vous générez un nouveau certificat lors de l'installation du serveur, les agents OfficeScan ne peuvent pas authentifier les communications provenant du serveur, car ils utilisent toujours l'ancien certificat (qui n'existe plus).

Pour plus d'informations sur la sauvegarde, la restauration, l'exportation et l'importation de certificats, voir *Utilisation du gestionnaire de certificats d'authentification à la page 13-53*.

Configuration de l'authentification des communications provenant du serveur

Procédure

1. Sur le serveur OfficeScan, accédez au répertoire <dossier_installation_serveur>\PCCSRV et ouvrez le fichier `ofcscan.ini` à l'aide d'un éditeur de texte.

2. Ajoutez ou modifiez la chaîne de texte `SGNF` de la section `[Global Settings]`.

   Pour activer l'authentification : `SGNF=1`

   Pour désactiver l'authentification : `SGNF=0`

   Remarque

   OfficeScan active par défaut l'authentification. Ajoutez la clé `SGNF` au fichier `ofcscan.ini` uniquement si vous souhaitez désactiver cette fonctionnalité.

3. Dans la console Web, accédez à **Agents** > **Paramètres de l'agent général** et cliquez sur **Enregistrer** pour déployer le paramètre sur tous les agents.

Utilisation du gestionnaire de certificats d'authentification

Le serveur OfficeScan conserve les certificats expirés pour les agents dont les clés publiques ont expiré. En effet, lorsque des agents ne se sont pas connectés au serveur pendant une période relativement longue, leurs clés publiques expirent. Lorsqu'ils se connectent à nouveau, ils associent leur clé publique au certificat expiré, ce qui leur permet de reconnaître les communications provenant du serveur. Le serveur déploie alors la clé publique la plus récente sur les agents.

Lors de la configuration des certificats, prenez en compte ce qui suit :

- Les lecteurs mappés et les chemins d'accès UNC sont acceptés pour indiquer le chemin d'accès d'un certificat.
- Choisissez un mot de passe sécurisé et conservez-en une trace pour référence future.



Important

Lors de l'utilisation de l'outil Gestionnaire de certificats d'authentification, tenez compte des exigences ci-dessous :

- L'utilisateur doit disposer de privilèges d'administrateur
- L'outil peut uniquement gérer les certificats situés sur le endpoint local

---

Procédure

1. Sur le serveur OfficeScan, ouvrez une invite de commandes et remplacez le répertoire existant par <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\CertificateManager`.

2. Lancez les commandes suivantes :

Commande	Exemple	Description
`CertificateManager.exe -c [Mot_de_passe_sauvegarde]`	`CertificateManager.exe -c strongpassword`	Génère un nouveau certificat Trend Micro et remplace l'ancien. Cette action est nécessaire si le certificat existant a expiré ou s'il a été révélé à des tiers non autorisés.
`CertificateManager.exe -b [Mot de passe] [Chemin d'accès du certificat]` **Remarque** Le certificat est au format ZIP.	`CertificateManager.exe -b strongpassword D:\Test\TrendMicro.zip`	Sauvegarde tous les certificats Trend Micro émis par le serveur OfficeScan actuel. Cette action est nécessaire pour sauvegarder le certificat sur le serveur OfficeScan. **Remarque** La sauvegarde des certificats du serveur OfficeScan vous permet de les utiliser au cas où vous devriez réinstaller le serveur OfficeScan.
`CertificateManager.exe -r [Mot de passe] [Chemin d'accès du certificat]` **Remarque** Le certificat est au format ZIP.	`CertificateManager.exe -r strongpassword D:\Test\TrendMicro.zip`	Restaure tous les certificats Trend Micro sur le serveur. Cette action est nécessaire pour restaurer le certificat sur un serveur OfficeScan réinstallé.

COMMANDE	EXEMPLE	DESCRIPTION
CertificateManager.exe -e [Chemin d'accès du certificat]	CertificateManager.exe -e <dossier_d'installation_de_l'agent>\OfcNTCer.dat	Exporte la clé publique de l'agent OfficeScan associée au certificat actuellement en cours d'utilisation. Cette action est nécessaire en cas de corruption de la clé publique utilisée par les agents. Copiez le fichier .dat dans le dossier racine de l'agent ; le fichier existant est par conséquent écrasé. **Important** Le chemin d'accès au fichier du certificat sur l'agent OfficeScan doit être le suivant : <dossier_d'installation_de_l'agent>\OfcNTCer.dat
CertificateManager.exe -i [Mot de passe] [Chemin d'accès du certificat] **Remarque** Le nom de fichier de certificat par défaut est le suivant : OfcNTCer.pfx	CertificateManager.exe -i strongpassword D:\Test\OfcNTCer.pfx	Importe un certificat Trend Micro dans le magasin de certificats.

Commande	Exemple	Description
CertificateManager.exe -l [Chemin d'accès au fichier CSV]	CertificateManager.exe -l D:\Test\MismatchedAgentList.csv	Répertorie (dans un fichier au format CSV) les agents utilisant actuellement un certificat ne correspondant pas.

Paramètres de la console Web

Utilisez l'écran **Paramètres de la console Web** pour :

- Configurez le serveur OfficeScan pour qu'il actualise le tableau de bord récapitulatif de façon périodique. Par défaut, le serveur actualise le tableau de bord toutes les 30 secondes. Le nombre de secondes peut varier entre 10 et 300.
- Définissez les paramètres de délai de la console Web. Par défaut, un utilisateur est automatiquement déconnecté de la console Web après 30 minutes d'inactivité. Le nombre de minutes peut être compris entre 10 et 60.

Configuration des paramètres de la console Web

Procédure

1. Accédez à **Administration** > **Paramètres** > **Console Web**.
2. Sélectionnez **Activer l'actualisation automatique**, puis sélectionnez l'intervalle d'actualisation.
3. Sélectionnez **Activer la déconnexion automatique de la console Web**, puis sélectionnez l'intervalle d'expiration.
4. Cliquez sur **Enregistrer**.

Gestionnaire de quarantaine

À chaque fois que l'agent OfficeScan détecte un risque de sécurité et que l'action de scan est la mise en quarantaine, il chiffre le fichier infecté, puis le déplace vers le dossier de quarantaine local situé dans le répertoire <*dossier d'installation de l'agent*>`\SUSPECT`.

Une fois le fichier déplacé dans le répertoire de quarantaine local, l'agent OfficeScan l'envoie vers le répertoire de quarantaine désigné. Spécifiez le répertoire dans l'onglet **Agents** > **Gestion des agents > Paramètres** > **Paramètre de {type de scan}** > **Action**. Les fichiers du répertoire de quarantaine désigné sont chiffrés pour les empêcher d'infecter d'autres fichiers. Voir la *Répertoire de quarantaine à la page 7-42* pour plus d'informations.

Si le répertoire de quarantaine désigné se trouve sur l'ordinateur du serveur OfficeScan, modifiez les paramètres du répertoire de quarantaine du serveur dans la console Web. Le serveur stocke les fichiers mis en quarantaine dans le répertoire <*dossier d'installation du serveur*>`\PCCSRV\Virus`.



Remarque

Si l'agent OfficeScan ne parvient pas à envoyer le fichier chiffré au serveur OfficeScan pour une raison quelconque, par exemple un problème de connexion réseau, le fichier chiffré reste dans le dossier de quarantaine de l'agent OfficeScan. L'agent OfficeScan tentera d'envoyer à nouveau le fichier lors de sa prochaine connexion au serveur OfficeScan.

Configuration des paramètres du répertoire de quarantaine

Procédure

1. Accédez à **Administration** > **Paramètres** > **Gestionnaire de quarantaine**.

2. Acceptez ou modifiez la capacité par défaut du dossier de quarantaine et la taille maximum d'un fichier infecté qu'OfficeScan peut stocker dans un dossier de quarantaine.

   Les valeurs par défaut s'affichent à l'écran.

3. Cliquez sur **Enregistrer les paramètres de mise en quarantaine**.

4. Pour supprimer tous les fichiers stockés dans le dossier de quarantaine, cliquez sur **Supprimer tous les fichiers en quarantaine**.

Server Tuner

Utilisez Server Tuner pour optimiser les performances du serveur OfficeScan en utilisant les paramètres pour les questions de performances liées au serveur OfficeScan suivantes :

- **Télécharger**

  Lorsque le nombre d'agents OfficeScan (y compris les agents de mise à jour) demandant des mises à jour au serveur OfficeScan excède les ressources disponibles du serveur, celui-ci place la demande de mise à jour de l'agent dans une file d'attente et traite les demandes lorsque les ressources deviennent à nouveau disponibles. Lorsqu'un agent réussit la mise à jour des composants à partir du serveur OfficeScan, il notifie ensuite le serveur de la fin de la mise à jour. Définissez le nombre maximal de minutes pendant lesquelles le serveur OfficeScan attend avant de recevoir une notification de mise à jour de l'agent. Définissez également le nombre maximal de tentatives de notification de l'agent par le serveur lui demandant d'exécuter une mise à jour et d'appliquer de nouveaux paramètres de configuration. Le serveur essaie uniquement de notifier l'agent s'il ne reçoit pas automatiquement de notification de celui-ci.

- **Buffer**

  Lorsque le serveur OfficeScan reçoit plusieurs demandes d'agents OfficeScan, par exemple des demandes de mise à jour, le serveur traite autant de demandes que possible, puis place les autres demandes dans une mémoire tampon. Le serveur traite alors individuellement les demandes enregistrées dans la mémoire tampon au fur et à mesure que des ressources se libèrent. Précisez la taille de la mémoire tampon pour des événements tels que des demandes de mise à jour des agents et la réception des journaux des agents.

- **Trafic réseau**

Le volume de trafic réseau varie pendant la journée. Pour contrôler le flux de trafic réseau vers le serveur OfficeScan et vers les autres sources de mises à jour, précisez le nombre d'agents OfficeScan qui peuvent se mettre à jour simultanément à un moment déterminé de la journée.

Serveur Tuner utilise le fichier suivant : `SvrTune.exe`

Exécution du Server Tuner

Procédure

1. Sur l'ordinateur du serveur OfficeScan, accédez au répertoire <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\SvrTune`.

2. Double-cliquez sur le fichier `SvrTune.exe` pour démarrer Server Tuner.

   La console Server Tuner s'ouvre.

3. Sous **Download**, modifiez les données suivantes :

   - **Délai d'attente pour le client** : Saisissez le délai (en minutes) pendant lequel le serveur OfficeScan attend de recevoir une réponse des agents concernant la mise à jour. Si l'agent ne répond pas dans ce délai, le serveur OfficeScan considère que l'agent ne dispose pas des composants actuels. Lorsqu'un agent notifié est hors délai, un espace devient disponible pour la notification d'un autre agent en attente.

   - **Délai d'attente pour l'agent de mise à jour** : Saisissez le délai (en nombre de minutes) pendant lequel le serveur OfficeScan attend de recevoir une réponse d'un agent de mise à jour concernant la mise à jour. Lorsqu'un agent notifié est hors délai, un espace devient disponible pour la notification d'un autre agent en attente.

   - **Retry count** : Saisissez le nombre maximal de fois que le serveur OfficeScan essaie de notifier un agent d'exécuter une mise à jour ou d'appliquer de nouveaux paramètres de configuration.

   - **Intervalle entre deux tentatives** : Saisissez le nombre de minutes d'attente du serveur OfficeScan entre deux tentatives de notification.

4. Sous **Buffer**, modifiez les données suivantes :

- **Mémoire tampon des événements** : Saisissez le nombre maximal de rapports d'événements d'agents destinés au serveur (concernant par exemple la mise à jour des composants) conservés par OfficeScan dans la mémoire tampon. La connexion à l'agent est interrompue pendant que la demande de l'agent est en attente dans la mémoire tampon. OfficeScan établit une connexion avec un agent lorsqu'il traite le rapport de cet agent et le supprime de la mémoire tampon.

- **Log Buffer** : Saisissez le nombre maximal de rapports d'informations de journal des agents destinés au serveur et conservées par OfficeScan dans la mémoire tampon. La connexion à l'agent est interrompue pendant que la demande de l'agent est en attente dans la mémoire tampon. OfficeScan établit une connexion avec un agent lorsqu'il traite le rapport de cet agent et le supprime de la mémoire tampon.



Remarque

Si un grand nombre d'agents communique avec votre serveur, augmentez la taille de la mémoire tampon. Une mémoire tampon de grande taille signifie toutefois une utilisation plus importante de la mémoire du serveur.

5. Sous **Network Traffic**, modifiez les données suivantes :

    - **Heures normales** : Cliquez sur les boutons d'option qui représentent les heures de la journée auxquelles vous considérez que le trafic réseau est normal.

    - **Heures creuses** : Cliquez sur les boutons d'option qui représentent les heures de la journée auxquelles vous considérez que le trafic réseau est à son plus bas niveau.

    - **Heures pleines** : Cliquez sur les boutons d'option qui représentent les heures de la journée auxquelles vous considérez que le trafic réseau est à son plus haut niveau.

    - **Connexions client maximum** : Saisissez le nombre maximum de clients qui peuvent simultanément mettre à jour des composants, depuis une autre source de mise à jour et depuis le serveur OfficeScan. Saisissez un nombre maximum de clients pour chaque période. Lorsque le nombre maximal de connexions est atteint, un agent OfficeScan ne peut mettre à jour des composants

qu'après la fermeture de la une connexion en cours d'un autre agent (soit lorsqu'une mise à jour est terminée, soit lorsque le délai de réponse de l'agent dépasse la limite spécifiée dans le champ **Délai d'attente pour le client** ou **Délai d'attente pour l'agent de mise à jour**).

6. Cliquez sur **OK**. Une invite apparaît vous demandant de relancer le service principal d'OfficeScan.



Remarque

Seul le service redémarre, pas l'ordinateur.

7. Sélectionnez l'une des options de redémarrage suivantes :

   - Cliquez sur **Oui** pour sauvegarder les paramètres de Server Tuner et relancer le service. Les paramètres prennent effet immédiatement après la relance.
   - Cliquez sur **Non** pour sauvegarder les paramètres de Server Tuner sans relancer le service. Redémarrez le service principal d'OfficeScan ou redémarrez l'ordinateur du serveur OfficeScan pour que les paramètres soient appliqués.

Smart Feedback

Trend Micro Smart Feedback partage les informations sur les menaces anonymes avec Smart Protection Network, ce qui permet à Trend Micro d'identifier rapidement les nouvelles menaces et d'y répondre. Vous pouvez désactiver Smart Feedback à tout moment via cette console.

Participation au programme Smart Feedback

Procédure

1. Accédez à **Administration** > **Smart Protection** > **Smart Feedback**.
2. Cliquez sur **Activer Trend Micro Smart Feedback**.

3. Pour aider Trend Micro à mieux connaître votre entreprise, sélectionnez son **secteur d'activité**.

4. Pour envoyer des informations sur des menaces de sécurité potentielles figurant dans les fichiers de vos agents OfficeScan, cochez la case **Activer les commentaires sur les fichiers programmes suspects**.



Remarque

Les fichiers envoyés à Smart Feedback ne contiennent pas de données utilisateur et ne sont utilisés que pour l'analyse des menaces.

5. Pour configurer les critères d'envoi de vos commentaires, sélectionnez le nombre de détections pour un laps de temps donné qui déclencheront cet envoi.

6. Pour réduire les risques d'interruption du réseau, indiquez la bande passante maximale qu'OfficeScan peut utiliser pour l'envoi des commentaires.

7. Cliquez sur **Enregistrer**.



Chapitre 14

Gestion de l'agent OfficeScan

Ce chapitre décrit la gestion et les configurations de l'agent OfficeScan.

Les rubriques sont les suivantes :

Emplacement de l'Endpoint

OfficeScan dispose d'une fonctionnalité de détection d'emplacement qui détermine si l'emplacement d'un agent OfficeScan est interne ou externe. La détection d'emplacement est utilisée par les fonctionnalités et services OfficeScan suivants :

Tableau 14-1. Fonctionnalités et services utilisant la détection d'emplacement

Fonctionnalité/ Service	Description
Services de réputation de sites Web	L'emplacement de l'agent OfficeScan détermine la stratégie de réputation de sites Web qui sera appliquée par l'agent OfficeScan. Les administrateurs appliquent généralement une stratégie plus stricte pour les agents externes. Pour obtenir des informations détaillées sur les stratégies de réputation de sites Web, voir *Stratégies de réputation de sites Web à la page 11-5*.
Services de File Reputation	Pour les agents utilisant Smart Scan, l'emplacement de l'agent OfficeScan détermine la source Smart Protection à laquelle les agents envoient des requêtes de scan. Les agents OfficeScan externes envoient des requêtes de scan à Smart Protection Network alors que les agents internes les envoient aux sources définies dans la liste de sources Smart Protection. Pour plus d'informations concernant les sources Smart Protection, voir *Sources Smart Protection à la page 4-6*.
Prévention contre la perte de données	L'emplacement d'un agent OfficeScan détermine la stratégie de prévention contre la perte de données appliquée par l'agent. Les administrateurs appliquent généralement une stratégie plus stricte pour les agents externes. Pour plus d'informations sur les stratégies Prévention contre la perte de données, consultez *Stratégies de prévention contre la perte de données à la page 10-3*.

FONCTIONNALITÉ/ SERVICE	DESCRIPTION
Contrôle des dispositifs	L'emplacement d'un agent OfficeScan détermine la stratégie de contrôle des dispositifs appliquée par l'agent. Les administrateurs appliquent généralement une stratégie plus stricte pour les agents externes. Pour plus d'informations concernant les stratégies de contrôle des dispositifs, voir *Contrôle des dispositifs à la page 9-2*.

Critères d'emplacement

Indiquez si l'emplacement est basé sur l'adresse IP de passerelle du endpoint de l'agent OfficeScan ou sur l'état de connexion de l'agent OfficeScan avec le serveur OfficeScan ou un serveur de référence.

- **État de la connexion de l'agent** : Si l'agent OfficeScan peut se connecter au serveur OfficeScan ou à l'un des serveurs de référence attribués sur l'intranet, l'emplacement de l'endpoint est interne. De plus, si un endpoint situé hors du réseau de l'entreprise peut se connecter au serveur OfficeScan/serveur de référence, son emplacement est également considéré comme étant interne. Si aucune de ces conditions ne s'applique, l'emplacement de l'endpoint est externe.
- **Adresses IP et MAC de passerelle** : L'emplacement d'un endpoint est interne si l'adresse IP de passerelle du endpoint de l'agent OfficeScan correspond à l'une des adresses IP de passerelle que vous spécifiez dans l'écran **Emplacement de l'Endpoint**. Si tel n'est pas le cas, l'emplacement de l'endpoint est externe.

Configuration des paramètres d'emplacement

Procédure

1. Accédez à **Agents** > **Emplacement de l'Endpoint**.
2. Indiquez si l'emplacement dépend du paramètre **État de la connexion de l'agent** ou **Adresses IP et MAC de passerelle**.

3. Si vous choisissez **État de la connexion de l'agent**, décidez si vous souhaitez utiliser un serveur de référence.

   Voir *Serveurs de référence à la page 13-30* pour obtenir des informations détaillées.

   a. Si aucun serveur de référence n'est spécifié, l'agent OfficeScan vérifie l'état de connexion avec le serveur OfficeScan lorsque les événements suivants se produisent :

      - L'agent OfficeScan passe du mode itinérance au mode normal (en ligne/hors ligne).
      - L'agent OfficeScan passe d'une méthode de scan à une autre. Voir *Types de méthodes de scan à la page 7-9* pour obtenir des informations détaillées.
      - L'agent OfficeScan détecte un changement d'adresse IP du endpoint.
      - L'agent OfficeScan redémarre.
      - Le serveur lance une vérification de connexion. Voir *Icônes de l'agent OfficeScan à la page 14-27* pour obtenir des informations détaillées.
      - Les critères d'emplacement de la réputation de sites Web changent lors de l'application des paramètres généraux.
      - La stratégie de prévention des épidémies n'est plus appliquée et les paramètres antérieurs à l'épidémie sont restaurés.

   b. Si un serveur de référence est spécifié, l'agent OfficeScan vérifie d'abord son état de connexion avec le serveur OfficeScan, puis avec le serveur de référence si la connexion au serveur OfficeScan a échoué. L'agent OfficeScan vérifie l'état de connexion toutes les heures, ainsi que lorsqu'un des événements ci-dessus se produit.

4. Si vous choisissez **Adresse IP de passerelle et adresse MAC** :

   a. Saisissez l'adresse IPv4/IPv6 de passerelle dans la zone de texte prévue à cet effet.

   b. Saisissez l'adresse MAC.

   c. Cliquez sur **Ajouter**.

Si vous ne saisissez pas d'adresse MAC, OfficeScan inclura toutes les adresses MAC appartenant à l'adresse IP spécifiée.

d. Répétez les étapes a à c jusqu'à ce que toutes les adresses IP de passerelle que vous souhaitez ajouter s'affichent.

e. Utilisez l'outil Gateway Settings Importer pour importer une liste de paramètres de passerelle.

Voir *Outil d'importation de paramètres de passerelle à la page 14-5* pour obtenir des informations détaillées.

5. Cliquez sur **Enregistrer**.

Outil d'importation de paramètres de passerelle

OfficeScan vérifie l'emplacement de l'endpoint pour déterminer la stratégie de réputation de sites Web à utiliser et la source Smart Protection auquel il doit se connecter. L'un des procédés employés par OfficeScan pour identifier l'emplacement consiste à vérifier l'adresse IP de passerelle et l'adresse MAC du endpoint.

Configurez les paramètres de passerelle sur l'écran **Emplacement de l'Endpoint** ou utilisez l'outil Gateway Settings Importer pour importer une liste de paramètres de passerelle vers l'écran **Emplacement de l'Endpoint**.

Utilisation de Gateway Settings Importer

Procédure

1. Préparez un fichier texte (`.txt`) contenant la liste des paramètres de passerelle. Sur chaque ligne, saisissez une adresse IPv4 ou IPv6 et éventuellement une adresse MAC.

Séparez les adresses IP des adresses MAC par une virgule. Le nombre maximum d'entrées est de 4096.

Par exemple :

```
10.1.111.222,00:17:31:06:e6:e7
```

```
2001:0db7:85a3:0000:0000:8a2e:0370:7334

10.1.111.224,00:17:31:06:e6:e7
```

2. Sur l'ordinateur du serveur, accédez au répertoire <*dossier d'installation du serveur*> `\PCCSRV\Admin\Utility\GatewaySettingsImporter` et double-cliquez sur `GSImporter.exe`.



Remarque

Vous ne pouvez pas exécuter l'outil Gateway Settings Importer à partir des services Terminal Services.

3. Sur l'écran **Outil d'importation de paramètres de passerelle**, accédez au fichier créé à l'étape 1 et cliquez sur **Importer**.

4. Cliquez sur **OK**.

   Les paramètres de passerelle s'affichent sur l'écran **Emplacement de l'Endpoint** et le serveur OfficeScan déploie les paramètres vers les agents OfficeScan.

5. Pour effacer toutes les entrées, cliquez sur **Effacer tout**.

   Si vous ne devez supprimer qu'une entrée particulière, faites-le à partir de l'écran **Emplacement de l'Endpoint**.

6. Pour exporter les paramètres vers un fichier, cliquez sur **Tout exporter**, puis spécifiez le nom et le type du fichier.

Gestion du programme de l'agent OfficeScan

Les rubriques suivantes traitent des moyens de gérer et de protéger le programme de l'agent OfficeScan :

- *Services de l'agent OfficeScan à la page 14-7*
- *Redémarrage des services de l'agent OfficeScan à la page 14-12*
- *Autoprotection de l'agent OfficeScan à la page 14-13*

- *Sécurité de l'agent OfficeScan à la page 14-17*
- *Restriction de l'accès à la console de l'agent OfficeScan à la page 14-18*
- *Déchargement et déverrouillage de l'agent OfficeScan à la page 14-20*
- *Privilège des agents OfficeScan itinérants à la page 14-21*
- *Agent Mover à la page 14-23*
- *Agents OfficeScan inactifs à la page 14-26*

Services de l'agent OfficeScan

L'agent OfficeScan exécute les services répertoriés dans le tableau suivant. Vous pouvez afficher l'état de ces services à partir de Microsoft Management Console.

TABLEAU 14-2. Services de l'agent OfficeScan

SERVICE	FONCTIONNALITÉS CONTRÔLÉES
Service de prévention des modifications non autorisées de Trend Micro (`TMBMSRV.exe`)	• Surveillance des comportements • Contrôle des dispositifs • Certified Safe Software Service
Pare-feu d'OfficeScan NT (`TmPfw.exe`)	Pare-feu OfficeScan
Service de protection des données OfficeScan (`dsagent.exe`)	• Prévention contre la perte de données • Contrôle des dispositifs
Service d'écoute d'OfficeScan NT (`tmlisten.exe`)	Communication entre l'agent OfficeScan et le serveur OfficeScan
Service proxy d'OfficeScan NT (`TmProxy.exe`)	• Réputation de sites Web • Scan de la messagerie POP3

Service	Fonctionnalités contrôlées
Service de scan en temps réel d'OfficeScanNT (`ntrtscan.exe`)	• Scan en temps réel • Scan programmé • Scan manuel/Scan immédiat
Structure de la solution client commune OfficeScan (`TmCCSF.exe`)	Service de protection avancé • Prévention contre l'exploitation du navigateur • Scan de la mémoire

Les services suivants fournissent une protection solide, mais leurs mécanismes de surveillance peuvent occuper les ressources système, en particulier sur les serveurs exécutant des applications exigeantes en ressources système :

- Service de prévention des modifications non autorisées de Trend Micro (`TMBMSRV.exe`)
- Pare-feu d'OfficeScan NT (`TmPfw.exe`)
- Service de protection des données OfficeScan (`dsagent.exe`)

C'est pour cela que ces services sont désactivés par défaut sur les plates-formes serveur (Windows Server 2003, Windows Server 2008 et Windows Server 2012). Si vous souhaitez activer ces services :

- Surveillez constamment les performances du système et effectuez les actions nécessaires lorsque vous remarquez une baisse de performances.
- Pour `TMBMSRV.exe`, vous pouvez activer le service si vous excluez les applications exigeantes en ressources système des stratégies de surveillance des comportements. Vous pouvez utiliser un outil d'optimisation des performances pour identifier les applications exigeantes en ressources système. Pour obtenir des informations détaillées, voir *Utilisation de Trend Micro Performance Tuning Tool à la page 14-10*.

Pour les plates-formes de poste de travail, ne désactivez les services que si vous remarquez une baisse significative des performances.

Activation ou désactivation des services de l'agent à partir de la console Web

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Pour les agents OfficeScan s'exécutant sous Windows XP, Vista, Windows 7, 8 ou 8.1 :
    a. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.

    > **Remarque**
    >
    > Lorsque vous sélectionnez le domaine racine ou des domaines spécifiques, le paramètre s'applique uniquement aux agents s'exécutant sous Windows XP, Vista, Windows 7, 8 ou 8.1. Le paramètre ne s'applique pas aux agents s'exécutant sous une plate-forme Windows Server, même s'ils appartiennent aux domaines.

    b. Cliquez sur **Paramètres** > **Paramètres des services complémentaires**.

    c. Cochez ou décochez la case dans les sections suivantes :
    - **Service de prévention des modifications non autorisées**
    - **Service de pare-feu**
    - **Service des connexions suspectes**
    - **Service de protection des données**
    - **Service de protection avancé**

    d. Cliquez sur **Enregistrer** pour appliquer les paramètres au(x) domaine(s). Si vous avez sélectionné l'icône du domaine racine, choisissez parmi les options suivantes :
    - **Appliquer à tous les agents** : Applique les paramètres à tous les agents s'exécutant sous Windows XP/Vista/Windows 7/8/8.1 existants et à

tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui ne sont pas encore créés au moment de la configuration des paramètres.

- **Appliquer aux domaines futurs uniquement** : Applique les paramètres uniquement aux agents s'exécutant sous Windows XP/Vista/ Windows 7/8/8.1 ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

3. Pour les agents OfficeScan s'exécutant sous Windows Server 2003, Windows Server 2008 ou Windows Server 2012 :

   a. Sélectionnez un seul agent dans l'arborescence des agents.

   b. Cliquez sur **Paramètres** > **Paramètres des services complémentaires**.

   c. Cochez ou décochez la case dans les sections suivantes :

      - **Service de prévention des modifications non autorisées**
      - **Service de pare-feu**
      - **Service des connexions suspectes**
      - **Service de protection des données**
      - **Service de protection avancé**

   d. Cliquez sur **Enregistrer**.

Utilisation de Trend Micro Performance Tuning Tool

Procédure

1. Téléchargez Trend Micro Performance Tuning Tool à partir de :

   http://esupport.trendmicro.com/solution/en-us/1056425.aspx

2. Décompressez `TMPerfTool.zip` pour extraire `TMPerfTool.exe`.

3. Placez `TMPerfTool.exe` dans le <*dossier d'installation de l'agent*> ou dans le même dossier que `TMBMCLI.dll`.

4. Cliquez avec le bouton droit de la souris sur `TMPerfTool.exe` et sélectionnez **Exécuter en tant qu'administrateur**.

5. Lisez et acceptez le contrat de licence utilisateur final puis cliquez sur **OK**.

6. Cliquez sur **Analyser**.

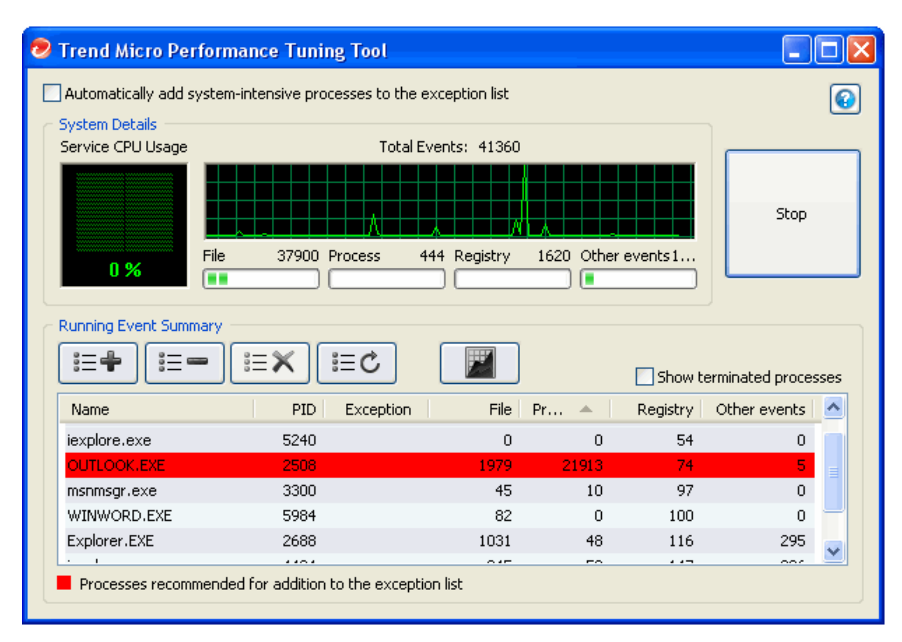


FIGURE 14-1. Processus exigeant en ressources système surligné

L'outil commence à surveiller l'utilisation de l'processeur et le chargement d'événements. Un processus exigeant en ressources système est surligné en rouge.

7. Sélectionnez un processus exigeant en ressources système puis cliquez sur le bouton **Ajouter à la liste d'exceptions (autoriser)** ( ).

8. Vérifiez si les performances du système ou des applications s'améliorent.

9. Si elles s'améliorent, sélectionnez à nouveau le processus, puis cliquez sur le bouton **Supprimer de la liste d'exceptions** ( ).

10. Si les performances baissent à nouveau, procédez comme suit :

    a. Notez le nom de l'application.

    b. Cliquez sur **Arrêter**.

    c. Cliquez sur le bouton **Générer le rapport** ( ), puis enregistrez le fichier `.xml`.

    d. Vérifiez les applications identifiées comme conflictuelles et ajoutez-les à la liste d'exceptions de surveillance des comportements.

    Pour obtenir des informations détaillées, voir *Liste d'exceptions de la surveillance des comportements à la page 8-6*.

Redémarrage des services de l'agent OfficeScan

OfficeScan redémarre les services de l'agent OfficeScan qui ont cessé de répondre de manière inattendue et n'ont pas été arrêtés par un processus système normal. Pour plus d'informations concernant les services de l'agent, voir *Services de l'agent OfficeScan à la page 14-7*.

Configurez les paramètres nécessaires pour permettre aux services de l'agent OfficeScan de redémarrer.

Configuration des paramètres de redémarrage des services

Procédure

1. Accédez à **Agents** > **Paramètres généraux de l'agent**.

2. Allez à la section **Redémarrage du service d'OfficeScan**.

3. Sélectionnez **Redémarrer automatiquement un service de l'agent OfficeScan s'il s'interrompt de façon inattendue**.

4. Configurez les éléments suivants :

- **Redémarrer le service après ____ minutes** : Indiquez le temps (en minutes) devant s'écouler avant qu'OfficeScan ne redémarre un service.
- **Si la première tentative de redémarrage du service échoue, réessayer __ fois** : Spécifiez le nombre maximum de nouvelles tentatives pour le redémarrage d'un service. Redémarrez manuellement un service s'il reste arrêté après le nombre maximum de nouvelles tentatives.
- **Remettre à zéro le compte d'échecs de redémarrage après __ heures** : Si un service reste arrêté une fois que le nombre maximum de nouvelles tentatives a été épuisé, OfficeScan attend un certain nombre d'heures avant de réinitialiser le compte d'échecs. Si un service reste arrêté une fois que le nombre d'heures est écoulé, OfficeScan le redémarre.

Autoprotection de l'agent OfficeScan

L'autoprotection de l'agent fournit à l'agent OfficeScan des moyens de protéger les processus et autres ressources nécessaires à un fonctionnement correct. L'autoprotection de l'agent OfficeScan permet de contrecarrer les tentatives de désactivation de la protection contre les programmes malveillants, qu'elles proviennent de programmes ou d'utilisateurs.

L'autoprotection de l'agent OfficeScan fournit les options suivantes :

- *Protéger les services de l'agent OfficeScan à la page 14-14*
- *Protéger les fichiers du dossier d'installation de l'agent OfficeScan à la page 14-15*
- *Protéger les clés de Registre de l'agent OfficeScan à la page 14-16*
- *Protéger les processus de l'agent OfficeScan à la page 14-16*

Configuration des paramètres de l'autoprotection de l'agent OfficeScan

Procédure

1. Accédez à **Agents** > **Gestion des agents**.

2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.

3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.

4. Cliquez sur l'onglet **Autres paramètres** et accédez à la section **Autoprotection de l'agent OfficeScan**.

5. Activez les options suivantes :

    - *Protéger les services de l'agent OfficeScan à la page 14-14*
    - *Protéger les fichiers du dossier d'installation de l'agent OfficeScan à la page 14-15*
    - *Protéger les clés de Registre de l'agent OfficeScan à la page 14-16*
    - *Protéger les processus de l'agent OfficeScan à la page 14-16*

6. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :

    - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.
    - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Protéger les services de l'agent OfficeScan

OfficeScan bloque toutes les tentatives visant à mettre fin aux services de l'agent OfficeScan suivants :

- Service d'écoute d'OfficeScan NT (`TmListen.exe`)
- Service de scan en temps réel d'OfficeScanNT (`NTRtScan.exe`)
- Service proxy d'OfficeScan NT (`TmProxy.exe`)

- Pare-feu d'OfficeScan NT (`TmPfw.exe`)
- Service de protection des données OfficeScan (`dsagent.exe`)
- Service de prévention des modifications non autorisées de Trend Micro (`TMBMSRV.exe`)



Remarque

Si cette option est activée, OfficeScan peut empêcher l'installation de produits tiers sur les endpoints. Si vous rencontrez ce problème, vous pouvez désactiver temporairement l'option, puis la réactiver une fois le produit tiers installé.

- Structure de la solution client commune Trend Micro (`TmCCSF.exe`)

Protéger les fichiers du dossier d'installation de l'agent OfficeScan

Pour empêcher d'autres programmes ou l'utilisateur de modifier ou de supprimer des fichiers de l'agent OfficeScan, OfficeScan verrouille les fichiers suivants dans le <*dossier d'installation de l'agent*> racine :

- Tous les fichiers signés numériquement possédant les extensions `.exe`, `.dll` et `.sys`
- Certains fichiers sans signature numérique, dont :
  - `bspatch.exe`
  - `bzip2.exe`
  - `INETWH32.dll`
  - `libcurl.dll`
  - `libeay32.dll`
  - `libMsgUtilExt.mt.dll`
  - `msvcm80.dll`
  - `MSVCP60.DLL`

- `msvcp80.dll`
- `msvcr80.dll`
- `OfceSCV.dll`
- `OFCESCVPack.exe`
- `patchbld.dll`
- `patchw32.dll`
- `patchw64.dll`
- `PiReg.exe`
- `ssleay32.dll`
- `Tmeng.dll`
- `TMNotify.dll`
- `zlibwapi.dll`

Protéger les clés de Registre de l'agent OfficeScan

OfficeScan bloque toutes les tentatives de modification, suppression ou ajout de nouvelles entrées sous les clés et sous-clés de registre suivantes :

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Osprey`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\AMSP`

Protéger les processus de l'agent OfficeScan

OfficeScan bloque toutes les tentatives visant à mettre fin aux processus suivants :

- `TmListen.exe`: reçoit des commandes et des notifications depuis le serveur OfficeScan et facilite la communication entre l'agent OfficeScan et le serveur.
- `NTRtScan.exe`: effectue des scans en temps réel, programmés et manuels sur les agents OfficeScan
- `TmProxy.exe`: Scanne le trafic réseau avant que celui-ci ne puisse atteindre l'application cible
- `TmPfw.exe`: offre des fonctions de pare-feu au niveau des paquets, de recherche de virus de réseau et de détection d'intrusions.
- `TMBMSRV.exe`: Régule l'accès aux périphériques de stockage externes et empêche la modification non autorisée des clés de registre et des processus
- `DSAgent.exe`: Surveille la transmission de données sensibles et contrôle l'accès aux périphériques
- `PccNTMon.exe` : ce processus est responsable du lancement de la console de l'agent OfficeScan.
- `TmCCSF.exe` : effectue la prévention contre l'exploitation du navigateur et le scan de la mémoire.

Sécurité de l'agent OfficeScan

Contrôlez l'accès des utilisateurs aux paramètres du Registre et eu répertoire d'installation de l'agent OfficeScan en sélectionnant l'un des deux paramètres de sécurité disponibles.

Contrôle de l'accès au répertoire d'installation et aux clés de Registre de l'agent OfficeScan

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.

3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.

4. Cliquez sur l'onglet **Autres paramètres** et accédez à la section **Paramètres de sécurité de l'agent**.

5. Sélectionnez l'une des autorisations d'accès suivantes :

    - **Élevé** : Le répertoire d'installation de l'agent OfficeScan hérite des droits du dossier `Program Files` et les entrées de Registre de l'agent OfficeScan héritent des autorisations de la clé `HKLM\Software`. Pour la plupart des configurations d'Active Directory, les utilisateurs "normaux" (qui ne disposent pas de privilèges d'administrateur) sont dès lors limités à un accès en lecture seule.

    - **Normal** : Cette autorisation donne à tous les utilisateurs (le groupe d'utilisateurs « Tous ») les pleins droits sur le répertoire du programme de l'agent OfficeScan et les entrées de Registre de l'agent OfficeScan.

6. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :

    - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.

    - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Restriction de l'accès à la console de l'agent OfficeScan

Ce paramètre désactive l'accès à la console de l'agent OfficeScan depuis la barre d'état système ou le menu Démarrer de Windows. Les utilisateurs ne peuvent alors accéder à la console de l'agent OfficeScan qu'en cliquant sur `PccNTMon.exe` dans le <*dossier d'installation de l'agent*>. Après avoir configuré ce paramètre, rechargez l'agent OfficeScan pour qu'il entre en vigueur.

Ce paramètre ne désactive pas l'agent OfficeScan. L'agent OfficeScan s'exécute en arrière-plan et continue d'assurer une protection contre les risques de sécurité.

Restriction de l'accès à la console de l'agent OfficeScan

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Cliquez sur l'onglet **Autres paramètres** et accédez à la section **Restriction de l'accès à l'agent OfficeScan**.
5. Sélectionnez **Ne pas autoriser les utilisateurs à accéder à la console de l'agent OfficeScan depuis la barre d'état système ou le menu Démarrer de Windows**.
6. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :
    - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.
    - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Déchargement et déverrouillage de l'agent OfficeScan

Le privilège de déchargement et de déverrouillage de l'agent OfficeScan autorise les utilisateurs à arrêter momentanément l'agent OfficeScan ou à accéder à certaines fonctionnalités avancées de la console Web, avec ou sans mot de passe.

Affectation du privilège de déchargement et de déverrouillage de l'agent

---

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Dans l'onglet **Privilèges**, accédez à la section **Décharger et déverrouiller**.
5. Pour autoriser le déchargement de l'agent OfficeScan sans mot de passe, sélectionnez **Aucun mot de passe n'est requis**.
   - Si un mot de passe est nécessaire, sélectionnez **Un mot de passe est requis**, saisissez un mot de passe et confirmez-le.
6. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :
   - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet

pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Privilège des agents OfficeScan itinérants

Accordez à certains utilisateurs le privilège des agents OfficeScan itinérants si les événements agent-serveur interfèrent avec les tâches des utilisateurs. Par exemple, un utilisateur qui donne fréquemment des présentations peut activer le mode itinérance avant de lancer une présentation pour empêcher le serveur OfficeScan de déployer les paramètres de l'agent OfficeScan et de lancer un scan sur l'agent OfficeScan.

Lorsque les agents OfficeScan sont en mode itinérance :

- Les agents OfficeScan n'envoient pas de journaux au serveur OfficeScan, même si la connexion entre le serveur et les agents est opérationnelle.
- Le serveur OfficeScan n'initie pas de tâches et ne déploie pas de paramètres des agents OfficeScan sur les agents, même si la connexion entre le serveur et les agents est opérationnelle.
- Les agents OfficeScan mettent à jour les composants s'ils peuvent se connecter à l'une de leurs sources de mises à jour. Ces sources peuvent être le serveur OfficeScan, des agents de mise à jour ou une source de mise à jour personnalisée.

  Les événements suivants déclenchent une mise à jour pour les agents itinérants :

  - L'utilisateur effectue une mise à jour manuelle.
  - La mise à jour automatique de l'agent s'exécute. Vous pouvez désactiver la mise à jour automatique de l'agent pour les agents itinérants. Pour obtenir des informations détaillées, voir *Désactivation de la mise à jour automatique de l'agent sur les agents itinérants à la page 14-22*.
  - Une mise à jour programmée s'exécute. Seuls les agents disposant des privilèges nécessaires peuvent exécuter des mises à jour programmées. Vous pouvez retirer ce privilège à tout moment. Pour obtenir des informations détaillées, voir *Retrait du privilège de mise à jour programmée sur les agents OfficeScan itinérants à la page 14-23*.

Affectation du privilège de mode itinérance de l'agent

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Dans l'onglet **Privilèges**, accédez à la section **Itinérance**.
5. Sélectionnez **Activer le mode itinérance**.
6. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :
    - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.
    - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Désactivation de la mise à jour automatique de l'agent sur les agents itinérants

Procédure

1. Accédez à **Mises à jour** > **Agents** > **Mise à jour automatique**.
2. Allez à la section **Mise à jour déclenchée par un événement**.
3. Désactivez **Inclure le ou les agents itinérants et hors ligne**.



Remarque

Cette option est automatiquement désactivée lorsque vous désactivez **Lancer la mise à jour des composants sur les agents immédiatement après le téléchargement d'un nouveau composant par le serveur OfficeScan**.

Retrait du privilège de mise à jour programmée sur les agents OfficeScan itinérants

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Dans l'onglet **Privilèges**, allez à la section **Privilèges de mise à jour des composants**.
5. Désactivez l'option **Activer/Désactiver les mises à jour programmées**.
6. Cliquez sur **Enregistrer**.

Agent Mover

Si vous disposez de plusieurs serveurs OfficeScan sur le réseau, utilisez l'outil Agent Mover pour transférer des agents OfficeScan d'un serveur OfficeScan vers un autre. Cet outil est particulièrement utile lorsque vous ajoutez un nouveau serveur OfficeScan au réseau, pour transférer des agents OfficeScan existants vers ce nouveau serveur.



Remarque

Les deux serveurs doivent posséder une version dans la même langue. Si vous utilisez Agent Mover pour déplacer un agent OfficeScan qui exécute une version antérieure vers un serveur utilisant la version actuelle, l'agent OfficeScan sera automatiquement mis à niveau.

Assurez-vous que le compte que vous utilisez a des privilèges d'administrateur avant d'utiliser cet outil.

Exécution d'Agent Mover

Procédure

1. Sur le serveur OfficeScan, accédez au répertoire <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\IpXfer`.
2. Copiez `IpXfer.exe` sur le endpoint de l'agent OfficeScan. Si le endpoint de l'agent OfficeScan s'exécute sur une plate-forme x64, copiez `IpXfer_x64.exe`.
3. Sur le endpoint de l'agent OfficeScan, ouvrez une invite de commandes et accédez au dossier dans lequel vous avez copié le fichier exécutable.
4. Exécutez Agent Mover à l'aide de la syntaxe suivante :

```
<nom du fichier exécutable> -s <nom du serveur> -p <port
d'écoute du serveur> -c <port d'écoute de l'agent> -d
<domaine ou hiérarchie de domaines> -e <emplacement et nom
de fichier du certificat>
```

TABLEAU 14-3. Paramètres d'Agent Mover

PARAMÈTRE	EXPLICATION
`<nom du fichier exécutable>`	`IpXfer.exe` ou `IpXfer_x64.exe`
`-s <nom du serveur>`	Nom du serveur OfficeScan de destination (serveur vers lequel l'agent OfficeScan doit être transféré)

Paramètre	Explication
-p <port d'écoute du serveur>	Port d'écoute (ou Port sécurisé) du serveur OfficeScan de destination. Pour afficher le port d'écoute sur la console Web OfficeScan, cliquez sur **Administration** > **Paramètres** > **Connexion de l'agent**.
-c <port d'écoute de l'agent>	Numéro de port utilisé par le endpoint de l'agent OfficeScan pour communiquer avec le serveur.
-d <domaine ou hiérarchie de domaines>	Domaine ou sous-domaine de l'arborescence des agents sous lequel l'agent sera regroupé. La hiérarchie des domaines doit indiquer le sous-domaine.
-e <emplacement et nom de fichier du certificat>	Importe un nouveau certificat d'authentification pour l'agent OfficeScan lors du processus de déplacement. Si ce paramètre n'est pas utilisé, l'agent OfficeScan récupère automatiquement le certificat d'authentification actuel depuis le nouveau serveur qui le gère. **Remarque** L'emplacement par défaut du certificat sur le serveur OfficeScan est le suivant : <*Dossier d'installation du serveur*>\PCCSRV\Pccnt\Common\OfcNTCer.dat. Lors de l'utilisation d'un certificat provenant d'une source autre qu'OfficeScan, assurez-vous que ce certificat est au format DER (Distinguished Encoding Rules).

Exemples :

```
ipXfer.exe -s Serveur01 -p 8080 -c 21112 -d Groupe de travail
```

```
ipXfer_x64.exe -s Serveur02 -p 8080 -c 21112 -d Groupe de travail\Groupe01
```

5. Pour vérifier que l'agent OfficeScan dépend maintenant de l'autre serveur, procédez comme suit :

a. Sur le endpoint de l'agent OfficeScan, cliquez avec le bouton droit de la souris sur l'icône du programme de l'agent OfficeScan dans la barre d'état système.

b. Sélectionnez **Versions du composant**.

c. Vérifiez de quel serveur OfficeScan l'agent OfficeScan dépend dans le champ **Nom du serveur/port**.



Remarque

Si l'agent OfficeScan ne s'affiche pas dans l'arborescence des agents du nouveau serveur OfficeScan qui prendra en charge sa gestion, redémarrez le service principal du nouveau serveur (`ofservice.exe`).

Agents OfficeScan inactifs

Lorsque vous utilisez le programme de désinstallation de l'agent OfficeScan pour supprimer le programme de l'agent OfficeScan d'un endpoint, le serveur en est automatiquement informé. Dès qu'il reçoit cette notification, le serveur supprime l'icône de l'agent OfficeScan dans l'arborescence des agents, indiquant ainsi que cet agent n'existe plus.

En revanche, si vous utilisez d'autres méthodes pour désinstaller l'agent OfficeScan, telles que le reformatage du disque dur du endpoint ou la suppression manuelle des fichiers de l'agent OfficeScan, OfficeScan n'est pas informé de cette suppression et considère l'agent OfficeScan comme étant inactif. Lorsqu'un utilisateur décharge ou désactive l'agent OfficeScan pendant une longue période, le serveur considère également l'agent OfficeScan comme étant inactif.

Pour que l'arborescence des agents affiche uniquement les agents actifs, configurez OfficeScan de telle sorte qu'il supprime automatiquement de l'arborescence tous les agents inactifs.

Suppression automatique des agents inactifs

Procédure

1. Accédez à **Administration** > **Paramètres** > **Agents inactifs**.

2. Sélectionnez **Activer la suppression automatique des agents inactifs**.

3. Précisez ensuite combien de jours doivent s'écouler avant qu'OfficeScan considère un agent OfficeScan comme étant inactif.

4. Cliquez sur **Enregistrer**.

Connexion agent-serveur

L'agent OfficeScan doit maintenir une connexion continue avec son serveur parent afin de pouvoir mettre à jour les composants, recevoir des notifications et appliquer des modifications à la configuration en temps et en heure. Les rubriques suivantes traitent des méthodes permettant de vérifier l'état de connexion de l'agent OfficeScan et de résoudre les problèmes de connexion :

- *Adresses IP des agents à la page 5-9*
- *Icônes de l'agent OfficeScan à la page 14-27*
- *Vérification de la connexion agent-serveur à la page 14-44*
- *Journaux de vérification de la connexion à la page 14-45*
- *Agents inaccessibles à la page 14-46*

Icônes de l'agent OfficeScan

L'icône de l'agent OfficeScan dans la barre d'état système fournit des conseils visuels qui indiquent l'état actuel de l'agent et invitent les utilisateurs à effectuer certaines actions. À un moment donné, l'icône présentera une combinaison des conseils visuels suivants.

Tableau 14-4. État de l'agent OfficeScan indiqué dans l'icône de l'agent OfficeScan

État de l'agent	Description	Conseil visuel
Connexion de l'agent au serveur OfficeScan	Les agents en ligne sont connectés au serveur OfficeScan. Le serveur peut initier des tâches et déployer des paramètres vers ces agents.	L'icône contient un symbole représentant un battement de cœur. La couleur de fond est une ombre de couleur bleue ou rouge, selon l'état du service de scan en temps réel.
	Les agents hors ligne sont déconnectés du serveur OfficeScan. Le serveur ne peut pas gérer ces agents.	L'icône contient un symbole représentant l'arrêt d'un battement de cœur. La couleur de fond est une ombre de couleur bleue ou rouge, selon l'état du service de scan en temps réel. Un agent a la possibilité de passer en mode hors ligne même s'il est connecté au réseau. Pour obtenir des informations sur ce problème, voir *Solutions aux problèmes indiqués par les icônes de l'agent OfficeScan à la page 14-41*.
	Les agents itinérants sont soit capables ou non de communiquer avec le serveur OfficeScan.	L'icône contient les symboles de bureau et de signal. La couleur de fond est une ombre de couleur bleue ou rouge, selon l'état du service de scan en temps réel. Pour plus d'informations sur les agents itinérants, voir *Privilège des agents OfficeScan itinérants à la page 14-21*.

ÉTAT DE L'AGENT	DESCRIPTION	CONSEIL VISUEL
Disponibilité des sources Smart Protection	Les sources Smart Protection incluent les serveurs Smart Protection Server et Trend Micro Smart Protection Network. Les agents de scan traditionnel se connectent aux sources Smart Protection pour les requêtes de réputation de sites Web. Les agents Smart Scan se connectent aux sources Smart Protection pour les requêtes de scan et de réputation de sites Web.	L'icône contient une coche si une source Smart Protection est disponible.
		L'icône contient une barre de progression si aucune source Smart Protection n'est disponible et que l'agent tente d'établir la connexion avec les sources. Pour obtenir des informations sur ce problème, voir *Solutions aux problèmes indiqués par les icônes de l'agent OfficeScan à la page 14-41*.
		Pour les agents de scan traditionnel, aucune coche ni barre de progression ne s'affiche si la réputation de sites Web a été désactivée.

État de l'agent	Description	Conseil visuel
État du service de scan en temps réel	OfficeScan utilise le service de scan en temps réel non seulement pour le scan en temps réel mais également pour les scans manuel et programmé. Le service doit être opérationnel, sinon l'agent devient vulnérable aux risques de sécurité.	Toute l'icône est ombrée en bleu si le service de scan en temps réel fonctionne. Deux nuances de bleu sont utilisées pour indiquer la méthode de scan de l'agent. • Pour le scan traditionnel : • Pour Smart Scan :
		Un ombrage rouge est appliqué à l'intégralité de l'icône si le service de scan en temps réel a été désactivé ou ne fonctionne pas. Deux nuances de rouge sont utilisées pour indiquer la méthode de scan de l'agent. • Pour le scan traditionnel : • Pour Smart Scan : Pour obtenir des informations sur ce problème, voir *Solutions aux problèmes indiqués par les icônes de l'agent OfficeScan à la page 14-41*.

ÉTAT DE L'AGENT	DESCRIPTION	CONSEIL VISUEL
État du scan en temps réel	Le scan en temps réel fournit une protection proactive en scannant les fichiers au moment où ils sont créés, modifiés ou récupérés, afin de détecter tout risque de sécurité.	Il n'y a pas de conseils visuels si le scan en temps réel est activé.
		Toute l'icône est entourée d'un cercle rouge et contient une ligne diagonale rouge si le scan en temps réel est désactivé. Pour obtenir des informations sur ce problème, voir *Solutions aux problèmes indiqués par les icônes de l'agent OfficeScan à la page 14-41*.
État de mise à jour du fichier de signatures	Les agents doivent mettre à jour régulièrement le fichier de signatures pour protéger l'agent contre les nouvelles menaces.	Il n'y a aucun conseil visuel si le fichier de signatures est à jour ou légèrement obsolète.
		L'icône contient un point d'exclamation si le fichier de signatures est largement obsolète. Cela signifie que le fichier de signatures n'a pas été mis à jour depuis longtemps. Pour plus d'informations sur les modalités de mise à jour des agents, voir *Mises à jour des agents OfficeScan à la page 6-31*.

Icônes Smart Scan

Les icônes suivantes peuvent s'afficher lorsque les agents OfficeScan utilisent Smart Scan.

Tableau 14-5. Icônes Smart Scan

Icône	Connexion avec le serveur OfficeScan	Disponibilité des sources Smart Protection	Service de scan en temps réel	Scan en temps réel
	En ligne	Disponible	Opérationnel	Activé
	En ligne	Disponible	Opérationnel	Désactivé
	En ligne	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel
	En ligne	Indisponible, reconnexion aux sources	Opérationnel	Activé
	En ligne	Indisponible, reconnexion aux sources	Opérationnel	Désactivé
	En ligne	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel
	Hors ligne	Disponible	Opérationnel	Activé
	Hors ligne	Disponible	Opérationnel	Désactivé
	Hors ligne	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel
	Hors ligne	Indisponible, reconnexion aux sources	Opérationnel	Activé
	Hors ligne	Indisponible, reconnexion aux sources	Opérationnel	Désactivé

Icône	Connexion avec le serveur OfficeScan	Disponibilité des sources Smart Protection	Service de scan en temps réel	Scan en temps réel
	Hors ligne	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel
	Itinérant	Disponible	Opérationnel	Activé
	Itinérant	Disponible	Opérationnel	Désactivé
	Itinérant	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel
	Itinérant	Indisponible, reconnexion aux sources	Opérationnel	Activé
	Itinérant	Indisponible, reconnexion aux sources	Opérationnel	Désactivé
	Itinérant	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel

Icônes de scan traditionnel

Les icônes suivantes peuvent s'afficher lorsque les agents OfficeScan utilisent le scan traditionnel.

TABLEAU 14-6. Icônes de scan traditionnel

ICÔNE	CONNEXION AVEC LE SERVEUR OFFICESCAN	SERVICES DE RÉPUTATION DE SITES WEB FOURNIS PAR LES SOURCES SMART PROTECTION	SERVICE DE SCAN EN TEMPS RÉEL	SCAN EN TEMPS RÉEL	FICHIER DE SIGNATURES DE VIRUS
	En ligne	Disponible	Opérationnel	Activé	À jour ou légèrement obsolète
	En ligne	Indisponible, reconnexion aux sources	Opérationnel	Activé	À jour ou légèrement obsolète
	En ligne	Disponible	Opérationnel	Activé	Largement obsolète
	En ligne	Indisponible, reconnexion aux sources	Opérationnel	Activé	Largement obsolète
	En ligne	Disponible	Opérationnel	Désactivé	À jour ou légèrement obsolète
	En ligne	Indisponible, reconnexion aux sources	Opérationnel	Désactivé	À jour ou légèrement obsolète
	En ligne	Disponible	Opérationnel	Désactivé	Largement obsolète
	En ligne	Indisponible, reconnexion aux sources	Opérationnel	Désactivé	Largement obsolète
	En ligne	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète

Icône	Connexion avec le serveur OfficeScan	Services de réputation de sites Web fournis par les sources Smart Protection	Service de scan en temps réel	Scan en temps réel	Fichier de signatures de virus
	En ligne	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète
	En ligne	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète
	En ligne	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète
	Hors ligne	Disponible	Opérationnel	Activé	À jour ou légèrement obsolète
	Hors ligne	Indisponible, reconnexion aux sources	Opérationnel	Activé	À jour ou légèrement obsolète
	Hors ligne	Disponible	Opérationnel	Activé	Largement obsolète
	Hors ligne	Indisponible, reconnexion aux sources	Opérationnel	Activé	Largement obsolète
	Hors ligne	Disponible	Opérationnel	Désactivé	À jour ou légèrement obsolète
	Hors ligne	Indisponible, reconnexion aux sources	Opérationnel	Désactivé	À jour ou légèrement obsolète
	Hors ligne	Disponible	Opérationnel	Désactivé	Largement obsolète

Icône	Connexion avec le serveur OfficeScan	Services de réputation de sites Web fournis par les sources Smart Protection	Service de scan en temps réel	Scan en temps réel	Fichier de signatures de virus
	Hors ligne	Indisponible, reconnexion aux sources	Opérationnel	Désactivé	Largement obsolète
	Hors ligne	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète
	Hors ligne	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète
	Hors ligne	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète
	Hors ligne	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète
	Itinérant	Disponible	Opérationnel	Activé	À jour ou légèrement obsolète
	Itinérant	Indisponible, reconnexion aux sources	Opérationnel	Activé	À jour ou légèrement obsolète
	Itinérant	Disponible	Opérationnel	Activé	Largement obsolète
	Itinérant	Indisponible, reconnexion aux sources	Opérationnel	Activé	Largement obsolète

Icône	Connexion avec le serveur OfficeScan	Services de réputation de sites Web fournis par les sources Smart Protection	Service de scan en temps réel	Scan en temps réel	Fichier de signatures de virus
	Itinérant	Disponible	Opérationnel	Désactivé	À jour ou légèrement obsolète
	Itinérant	Indisponible, reconnexion aux sources	Opérationnel	Désactivé	À jour ou légèrement obsolète
	Itinérant	Disponible	Opérationnel	Désactivé	Largement obsolète
	Itinérant	Indisponible, reconnexion aux sources	Opérationnel	Désactivé	Largement obsolète
	Itinérant	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète
	Itinérant	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète
	Itinérant	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète
	Itinérant	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète
	En ligne	Sans objet (fonctionnalité de réputation de sites Web désactivée sur l'agent)	Opérationnel	Activé	À jour ou légèrement obsolète

Icône	Connexion avec le serveur OfficeScan	Services de réputation de sites Web fournis par les sources Smart Protection	Service de scan en temps réel	Scan en temps réel	Fichier de signatures de virus
	En ligne	Sans objet (fonctionnalité de réputation de sites Web désactivée sur l'agent)	Opérationnel	Activé	Largement obsolète
	En ligne	Sans objet (fonctionnalité de réputation de sites Web désactivée sur l'agent)	Opérationnel	Désactivé	À jour ou légèrement obsolète
	En ligne	Sans objet (fonctionnalité de réputation de sites Web désactivée sur l'agent)	Opérationnel	Désactivé	Largement obsolète
	En ligne	Sans objet (fonctionnalité de réputation de sites Web désactivée sur l'agent)	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète
	En ligne	Sans objet (fonctionnalité de réputation de sites Web désactivée sur l'agent)	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète

Icône	Connexion avec le serveur OfficeScan	Services de réputation de sites Web fournis par les sources Smart Protection	Service de scan en temps réel	Scan en temps réel	Fichier de signatures de virus
	Hors ligne	Sans objet (fonctionnalité de réputation de sites Web désactivée sur l'agent)	Opérationnel	Activé	À jour ou légèrement obsolète
	Hors ligne	Sans objet (fonctionnalité de réputation de sites Web désactivée sur l'agent)	Opérationnel	Activé	Largement obsolète
	Hors ligne	Sans objet (fonctionnalité de réputation de sites Web désactivée sur l'agent)	Opérationnel	Désactivé	À jour ou légèrement obsolète
	Hors ligne	Sans objet (fonctionnalité de réputation de sites Web désactivée sur l'agent)	Opérationnel	Désactivé	Largement obsolète
	Hors ligne	Sans objet (fonctionnalité de réputation de sites Web désactivée sur l'agent)	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète

Icône	Connexion avec le serveur OfficeScan	Services de réputation de sites Web fournis par les sources Smart Protection	Service de scan en temps réel	Scan en temps réel	Fichier de signatures de virus
	Hors ligne	Sans objet (fonctionnalité de réputation de sites Web désactivée sur l'agent)	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète
	Itinérant	Sans objet (fonctionnalité de réputation de sites Web désactivée sur l'agent)	Opérationnel	Activé	À jour ou légèrement obsolète
	Itinérant	Sans objet (fonctionnalité de réputation de sites Web désactivée sur l'agent)	Opérationnel	Activé	Largement obsolète
	Itinérant	Sans objet (fonctionnalité de réputation de sites Web désactivée sur l'agent)	Opérationnel	Désactivé	À jour ou légèrement obsolète
	Itinérant	Sans objet (fonctionnalité de réputation de sites Web désactivée sur l'agent)	Opérationnel	Désactivé	Largement obsolète

ICÔN E	CONNEXION AVEC LE SERVEUR OFFICESCAN	SERVICES DE RÉPUTATION DE SITES WEB FOURNIS PAR LES SOURCES SMART PROTECTION	SERVICE DE SCAN EN TEMPS RÉEL	SCAN EN TEMPS RÉEL	FICHIER DE SIGNATURES DE VIRUS
	Itinérant	Sans objet (fonctionnalité de réputation de sites Web désactivée sur l'agent)	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète
	Itinérant	Sans objet (fonctionnalité de réputation de sites Web désactivée sur l'agent)	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète

Solutions aux problèmes indiqués par les icônes de l'agent OfficeScan

Exécutez les actions nécessaires lorsque l'icône de l'agent OfficeScan signale l'une des situations suivantes :

CONDITION	DESCRIPTION
Le fichier de signatures n'a pas été mis à jour depuis un certain temps	Les utilisateurs des agents OfficeScan doivent mettre à jour les composants. Depuis la console Web, vous pouvez configurer les paramètres de mise à jour des composants dans **Mises à jour** > **Agents** > **Mise à jour automatique** ou accorder aux utilisateurs le privilège de mise à jour dans **Agents** > **Gestion des agents >** **Paramètres** > **Privilèges et autres paramètres** > **Privilèges** > **Privilèges de mise à jour des composants**.
Le service de scan en temps réel a été désactivé ou ne fonctionne pas	Si le service de scan en temps réel (OfficeScan NT RealTime Scan) a été désactivé ou ne fonctionne plus, les utilisateurs doivent démarrer le service manuellement à partir de Microsoft Management Console.

Condition	Description
Scan en temps réel désactivé	Activez le scan en temps réel depuis la console Web (**Agents** > **Gestion des agents > Paramètres** > **Paramètres de scan** > **Paramètres de scan en temps réel**).
Scan en temps réel désactivé et agent OfficeScan en mode itinérant	Les utilisateurs doivent d'abord désactiver le mode itinérance. Après la désactivation du mode itinérance, activez le scan en temps réel depuis la console Web.
Un agent OfficeScan est connecté au réseau, mais apparaît hors ligne	Vérifiez la connexion depuis la console Web (**Journaux** > **Agents** > **Vérification de la connexion**), puis examinez les journaux de vérification de la connexion (**Journaux** > **Agents** > **Vérification de la connexion**). Si l'agent OfficeScan est toujours hors ligne après la vérification : 1. Si l'état de la connexion est hors ligne à la fois sur le serveur et sur l'agent OfficeScan, vérifiez la connexion réseau. 2. Si l'état de la connexion est hors ligne sur l'agent OfficeScan et en ligne sur le serveur, le nom de domaine du serveur peut avoir été modifié et l'agent OfficeScan se connecte au serveur à l'aide du nom de domaine (si vous avez sélectionné le nom de domaine au cours de l'installation du serveur). Enregistrez le nom de domaine du serveur OfficeScan sur le serveur DNS ou WINS ou ajoutez le nom de domaine et les données IP dans le fichier « hosts » du dossier `<dossier Windows>\system32\drivers\etc` du endpoint de l'agent. 3. Si l'état de la connexion sur l'agent OfficeScan est en ligne alors qu'il est hors ligne sur le serveur, vérifiez les paramètres de pare-feu OfficeScan. Le pare-feu risque de bloquer la communication serveur-agent, mais autorise la communication agent-serveur. 4. Si l'état de la connexion sur l'agent OfficeScan est en ligne alors qu'il est hors ligne sur le serveur, l'adresse IP de l'agent OfficeScan peut avoir été modifiée, mais son état n'apparaît pas sur le serveur (par exemple, lorsque l'agent est rechargé). Essayez de redéployer l'agent OfficeScan.

<table>
<tr><th>Condition</th><th>Description</th></tr>
<tr><td>Les sources Smart Protection ne sont pas disponibles</td><td>Effectuez ces tâches si un agent perd la connexion avec les sources Smart Protection :
1. Sur la console Web, accédez à l'écran Emplacement de l'Endpoint (Agents > Emplacement de l'Endpoint) et vérifiez si les paramètres suivants d'emplacement de l'endpoint ont été configurés correctement :
• Serveurs de référence et numéros de port
• Adresses IP de passerelle
2. Sur la console Web, accédez à l'écran Source Smart Protection (Administration > Smart Protection > Sources Smart Protection), puis procédez comme suit :
a. Vérifiez si les paramètres du serveur Smart Protection Server dans la liste standard ou personnalisée des sources sont corrects.
b. Vérifiez si la connexion aux serveurs peut être établie.
c. Cliquez sur Notifier tous les agents après avoir configuré la liste des sources.
3. Vérifiez que les fichiers de configuration suivants sont synchronisés sur le serveur Smart Protection Server et sur l'agent OfficeScan :
• <code>sscfg.ini</code>
• <code>ssnotify.ini</code>
4. Ouvrez l'Éditeur de Registre et vérifiez que l'agent est connecté au réseau d'entreprise.
Clé :
<code>HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\iCRC Scan\Scan Server</code>
• Si <code>LocationProfile=1</code>, l'agent OfficeScan est connecté au réseau et doit pouvoir se connecter au serveur Smart Protection Server.
• Si <code>LocationProfile=2</code>, l'agent OfficeScan n'est pas connecté au réseau et doit pouvoir se connecter à Smart</td></tr>
</table>

Condition	Description
	Protection Network. Dans Internet Explorer, vérifiez que le endpoint de l'agent OfficeScan peut naviguer sur des pages Web. 5. Vérifiez les paramètres proxy internes et externes utilisés pour la connexion à Smart Protection Network et aux serveurs Smart Protection Server. Pour obtenir des informations détaillées, voir *Proxy interne pour les agents OfficeScan à la page 14-51* et *Proxy externe pour les agents OfficeScan à la page 14-52*. 6. Pour les agents de scan traditionnel, assurez-vous que le service proxy d'OfficeScan NT (`TmProxy.exe`) est en cours d'exécution. Si ce service s'arrête, les agents ne peuvent pas se connecter aux sources Smart Protection pour la réputation de sites Web.

Vérification de la connexion agent-serveur

L'état de la connexion de l'agent au serveur OfficeScan s'affiche dans l'arborescence des agents de la console Web OfficeScan.

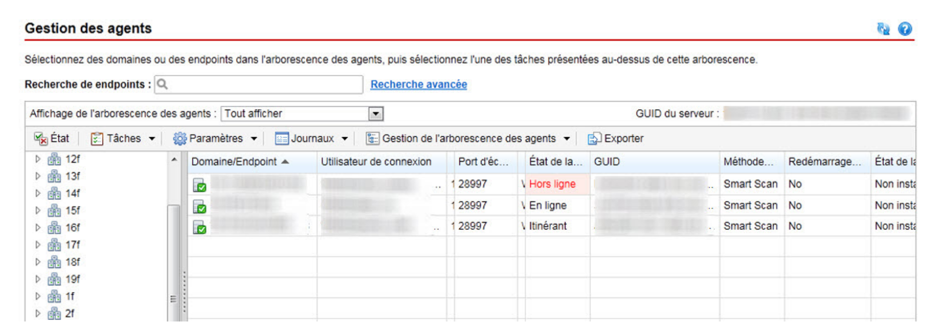


Figure 14-2. Arborescence des agents affichant l'état de la connexion de l'agent au serveur OfficeScan

Dans certains cas, l'affichage de l'état correct de la connexion de l'agent dans l'arborescence des agents est impossible. Par exemple, si vous débranchez accidentellement le câble réseau du endpoint d'un agent, cet agent ne peut pas informer

le serveur de son état hors ligne. Cet agent apparaîtra comme étant encore en ligne dans l'arborescence des agents.

Vérifiez la connexion agent -serveur manuellement ou laissez OfficeScan effectuer la vérification programmée. Vous ne pouvez pas sélectionner de domaines ni d'agents spécifiques, puis vérifier leur état de connexion. OfficeScan vérifie l'état de la connexion de tous les agents enregistrés auprès de lui.

Vérification des connexions agents-serveur

Procédure

1. Accédez à **Journaux** > **Agents** > **Vérification de la connexion**.
2. Pour vérifier manuellement la connexion agent-serveur, accédez à l'onglet **Vérification manuelle** et cliquez sur **Vérifier maintenant**.
3. Pour vérifier automatiquement la connexion agent-serveur, cliquez sur l'onglet **Vérification programmée**.
    a. Sélectionnez **Activer la vérification programmée**.
    b. Sélectionnez la fréquence et l'heure de début de la vérification.
    c. Cliquez sur **Enregistrer** pour enregistrer la programmation de vérification établie.
4. Vérifiez l'arborescence des agents pour contrôler l'état ou consulter les journaux de vérification de la connexion.

Journaux de vérification de la connexion

OfficeScan conserve les journaux de vérification de la connexion pour vous permettre de déterminer si le serveur OfficeScan peut ou non communiquer avec tous les agents enregistrés auprès de lui. OfficeScan crée une entrée de journal à chaque fois que vous vérifiez la connexion agent-serveur depuis la console Web.

Pour éviter que les journaux n'occupent trop d'espace sur votre disque dur, vous pouvez les supprimer manuellement ou configurer leur suppression programmée. Voir *Gestion du*

journal à la page 13-36 pour obtenir des informations complémentaires sur la gestion des journaux.

Affichage des journaux de vérification de la connexion

Procédure

1. Accédez à **Journaux** > **Agents** > **Vérification de la connexion**.
2. Consultez le résultat de vérification de la connexion en vérifiant la colonne **État**.
3. Pour sauvegarder les journaux dans un fichier `CSV` (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Agents inaccessibles

Les agents OfficeScan qui se trouvent sur des réseaux inaccessibles, tels que ceux situés sur des segments du réseau derrière une passerelle NAT, sont presque toujours hors ligne, car le serveur ne peut pas établir une connexion directe avec eux. Par conséquent, le serveur ne peut pas demander à ces agents d'effectuer les actions suivantes :

- Télécharger des derniers composants.
- Appliquer les paramètres de l'agent configurés sur la console Web. Par exemple, lorsque vous changez la fréquence du scan programmé sur la console Web, le serveur avertit immédiatement les agents d'appliquer le nouveau paramètre.

Par conséquent, les agents inaccessibles ne peuvent pas effectuer ces tâches en temps et en heure. Ils n'effectuent ces tâches que lorsqu'ils établissent la connexion avec le serveur, ce qui se produit lorsque :

- Ils s'enregistrent sur le serveur après l'installation.
- Ils redémarrent ou se rechargent. Cet événement ne se produit pas fréquemment et nécessite généralement l'intervention de l'utilisateur.
- Une mise à jour manuelle ou programmée est déclenchée sur l'agent. Cet événement ne se produit pas fréquemment non plus.

Le serveur n'est informé de la connectivité des agents et ne les traite comme étant en ligne que lors de l'enregistrement, du redémarrage ou du rechargement. Toutefois, du fait que le serveur n'est toujours pas en mesure d'établir la connexion avec les agents, il change immédiatement leur état pour les traiter comme étant hors ligne.

OfficeScan offre les fonctions de « battement de cœur » et d'interrogation du serveur pour résoudre les problèmes liés aux agents inaccessibles. Grâce ces fonctions, le serveur cesse de notifier les agents des mises à jour de composants et des changements de paramètres. À la place, le serveur prend un rôle passif, attendant toujours que les agents envoient le battement de cœur ou lancent l'interrogation. Lorsque le serveur détecte l'un de ces événements, il traite les agents comme étant en ligne.



Remarque

Les événements initiés par les agents qui ne sont pas associés au battement de cœur ou à l'interrogation du serveur, par exemple la mise à jour manuelle des agents et l'envoi de journaux, ne déclenchent pas la mise à jour par le serveur de l'état inaccessible des agents.

Battement de cœur

Des agents OfficeScan envoient des messages de battement de cœur pour prévenir le serveur que la connexion à partir de l'agent reste fonctionnelle. Lorsqu'il reçoit un message de battement de cœur, le serveur traite l'agent comme étant en ligne. Dans l'arborescence des agents, l'état de l'agent peut être :

- **En ligne** : Pour les agents ordinaires en ligne
- **Inaccessible/en ligne** : Pour les agents en ligne se trouvant sur le réseau inaccessible



Remarque

Les agents OfficeScan ne mettent pas à jour les composants et n'appliquent pas les nouveaux paramètres lors de l'envoi de messages de battement de cœur. Les agents ordinaires réalisent ces opérations durant les mises à jour de routine (voir *Mises à jour des agents OfficeScan à la page 6-31*). Les agents se trouvant sur le réseau inaccessible effectuent ces tâches au cours de l'interrogation du serveur.

La fonction de battement de cœur résout le problème des agents OfficeScan se trouvant sur des réseaux inaccessibles et apparaissant toujours comme étant hors ligne bien qu'ils puissent se connecter au serveur.

Un paramètre de la console Web contrôle la fréquence à laquelle les agents envoient des messages de battement de cœur. Si le serveur n'a pas reçu de battement de cœur, il ne traite pas immédiatement l'agent comme étant hors ligne. Un autre paramètre contrôle la durée sans battement de cœur devant s'écouler avant de faire passer l'état de l'agent à :

- **Hors ligne** : Pour les agents OfficeScan ordinaires hors ligne
- **Inaccessible/hors ligne** : Pour les agents OfficeScan hors ligne se trouvant sur le réseau inaccessible

Lorsque vous choisissez une configuration de battement de cœur, il s'agit de trouver le juste équilibre entre la nécessité d'afficher les informations les plus récentes sur l'état de l'agent et celle de gérer les ressources système. Le paramètre par défaut est satisfaisant dans la plupart des situations. Cependant, tenez compte des points suivants lorsque vous personnalisez la configuration des battements de cœur :

TABLEAU 14-7. Recommandations relatives aux battements de cœur

FRÉQUENCE DU BATTEMENT DE CŒUR	RECOMMANDATION
Battements de cœur à intervalles longs (plus de 60 minutes)	Plus l'intervalle entre les battements de cœur est long, plus le nombre d'événements pouvant se produire avant que l'état de l'agent ne soit indiqué sur la console Web du serveur est élevé.
Battements de cœur à intervalles courts (moins de 60 minutes)	Les intervalles courts présentent un état de l'agent mieux actualisé mais peuvent consommer beaucoup de bande passante.

Interrogation du serveur

La fonctionnalité d'interrogation du serveur résout le problème des agents OfficeScan inaccessibles qui ne reçoivent pas les notifications en temps et en heure concernant les mises à jour de composants et les changements des paramètres des agents. Cette fonction est indépendante de la fonction battement de cœur.

Avec la fonction d'interrogation du serveur :

- Les agents OfficeScan établissent automatiquement la connexion au serveur OfficeScan à intervalles réguliers. Lorsque le serveur détecte l'interrogation, il traite les agents comme étant « Inaccessibles/en ligne ».
- Les agents OfficeScan se connectent à une ou plusieurs de leurs sources de mise à jour pour télécharger les éventuels composants mis à jour et appliquer les nouveaux paramètres des agents. Si le serveur OfficeScan ou un agent de mise à jour est la source de mise à jour principale, les agents obtiennent à la fois les composants et les nouveaux paramètres. Si la source n'est pas le serveur OfficeScan ni un agent de mise à jour, les agents obtiennent seulement les composants mis à jour, puis se connectent au serveur OfficeScan ou à l'agent de mise à jour pour obtenir les nouveaux paramètres.

Configuration des fonctions de battement de cœur et d'interrogation du serveur

---

Procédure

1. Accédez à **Agents** > **Paramètres généraux de l'agent**.
2. Allez sur la section **Réseau inaccessible**.
3. Configurez les paramètres de l'interrogation du serveur.

   Pour plus de détails sur l'interrogation du serveur, voir *Interrogation du serveur à la page 14-48*.

   a. Si le serveur OfficeScan possède à la fois une adresse IPv4 et IPv6, vous pouvez saisir une plage d'adresses IPv4 ainsi qu'un préfixe et une longueur IPv6.

      Saisissez une plage d'adresses IPv4 si le serveur est en IPv4 pur ou un préfixe et une longueur IPv6 si le serveur est en IPv6 pur.

      Lorsque l'adresse IP d'un agent correspond à l'une des adresses de la plage, cet agent applique les paramètres de battement de cœur et d'interrogation du serveur et ce dernier traite l'agent comme faisant partie d'un réseau inaccessible.



Remarque

Les agents ayant une adresse IPv4 peuvent se connecter à un serveur OfficeScan IPv4 pur ou à double pile.

Les agents ayant une adresse IPv6 peuvent se connecter à un serveur OfficeScan IPv6 pur ou à double pile.

Des agents à double pile peuvent se connecter à un serveur OfficeScan IPv4 pur, IPv6 pur ou à double pile.

b. Dans **Les agents interrogent le serveur pour obtenir les composants et paramètres mis à jour toutes les __ minute(s)**, indiquez la fréquence d'interrogation du serveur. Saisissez une valeur comprise entre 1 et 129600 minutes.



Conseil

Trend Micro recommande que la fréquence d'interrogation du serveur représente au moins trois fois la fréquence d'envoi du battement de cœur.

4. Configurez les paramètres de battement de cœur.

Pour plus d'informations sur la fonction battement de cœur, voir *Battement de cœur à la page 14-47*.

a. Sélectionnez **Autoriser les agents à envoyer un battement de cœur au serveur**.

b. Sélectionnez **Tous les agents** ou **Seuls les agents du réseau inaccessible**.

c. Dans **Les agents envoient un battement de cœur toutes les __ minutes**, indiquez la fréquence à laquelle les agents envoient un battement de cœur. Saisissez une valeur comprise entre 1 et 129600 minutes.

d. Dans **Un agent est hors ligne en l'absence d'un battement de cœur au bout de __ minutes**, indiquez la durée sans battement de cœur devant s'écouler avant que le serveur OfficeScan considère l'agent comme étant hors ligne. Saisissez une valeur comprise entre 1 et 129600 minutes.

5. Cliquez sur **Enregistrer**.

Paramètres proxy des agents OfficeScan

Configurez les agents OfficeScan pour qu'ils utilisent des paramètres proxy lors de la connexion aux serveurs internes et externes.

Proxy interne pour les agents OfficeScan

Les agents OfficeScan peuvent utiliser les paramètres proxy internes pour se connecter aux serveurs suivants du réseau :

- Serveur OfficeScan

  L'ordinateur serveur héberge le serveur OfficeScan et le serveur Smart Protection Server intégré. Les agents se connectent au serveur OfficeScan pour mettre à jour les composants, obtenir les paramètres de configuration et envoyer les journaux. Les agents OfficeScan se connectent au serveur Smart Protection Server intégré pour envoyer des requêtes de scan.

- serveurs Smart Protection Server

  Les serveurs Smart Protection Server comprennent tous les serveurs Smart Protection Server autonomes et les serveurs Smart Protection Server intégrés des autres serveurs OfficeScan. Les agents OfficeScan se connectent aux serveurs pour envoyer des requêtes de scan et de réputation de sites Web.

Configuration des paramètres proxy internes

Procédure

1. Accédez à **Administration** > **Paramètres** > **Proxy**.
2. Cliquez sur l'onglet **Proxy interne**.
3. Accédez à la section **Connexion de l'agent au serveur OfficeScan**.
   a. Sélectionnez **Utilisez les paramètres proxy suivants lorsque les agents se connectent au serveur OfficeScan**.

b. Indiquez le nom ou l'adresse IPv4/IPv6 et le numéro de port du serveur proxy.



Remarque

Indiquez un serveur proxy à double pile identifié par son nom d'hôte si vous disposez d'agents IPv4 et IPv6. Ceci est dû au fait que les paramètres de proxy interne sont des paramètres globaux. Si vous indiquez une adresse IPv4, les agents Pv6 ne peuvent pas se connecter au serveur proxy. Il en va de même pour agents IPv4.

c. Si le serveur proxy requiert une authentification, saisissez le nom d'utilisateur et le mot de passe, puis confirmez le mot de passe.

4. Accédez à la section **Connexion des agents à des serveurs Smart Protection Server autonomes**.

    a. Sélectionnez **Utilisez les paramètres proxy suivants lorsque des agents se connectent à des serveurs Smart Protection Server autonomes**.

    b. Indiquez le nom ou l'adresse IPv4/IPv6 et le numéro de port du serveur proxy.

    c. Si le serveur proxy requiert une authentification, saisissez le nom d'utilisateur et le mot de passe, puis confirmez le mot de passe.

5. Cliquez sur **Enregistrer**.

Proxy externe pour les agents OfficeScan

Le serveur OfficeScan et l'agent OfficeScan peuvent utiliser des paramètres proxy externe lorsqu'ils se connectent à des serveurs hébergés par Trend Micro. Cette rubrique présente les paramètres proxy externe pour les agents. Pour connaître les paramètres de proxy externe pour le serveur, voir *Proxy for OfficeScan Server Updates à la page 6-22*.

Les agents OfficeScan utilisent les paramètres proxy configurés dans Internet Explorer pour se connecter à Trend Micro Smart Protection Network. Si une authentification auprès du serveur proxy est nécessaire, les agents utiliseront les informations d'authentification du serveur proxy (ID utilisateur et mot de passe).

Configuration des informations d'authentification sur le serveur proxy

Procédure

1. Accédez à **Administration** > **Paramètres** > **Proxy**.
2. Cliquez sur l'onglet **Proxy externe**.
3. Accédez à la section **Connexion de l'agent OfficeScan aux serveurs Trend Micro**.
4. Saisissez l'ID utilisateur et le mot de passe nécessaires à l'authentification du serveur proxy. Les protocoles d'authentification sur le serveur proxy suivants sont pris en charge :
    - Authentification d'accès de base
    - Authentification d'accès Digest
    - Authentification intégrée de Windows
5. Cliquez sur **Enregistrer**.

Privilèges de configuration proxy pour les agents

Vous pouvez accorder aux utilisateurs d'agents l'autorisation de configurer les paramètres proxy. Les agents OfficeScan n'utilisent les paramètres proxy configurés par l'utilisateur que dans les cas suivants :

- Lorsque les agents OfficeScan exécutent l'option « Mettre à jour ».
- Lorsque les paramètres proxy automatiques sont désactivés par les utilisateurs ou que l'agent OfficeScan ne parvient pas à les détecter. Voir la*Paramètres proxy automatiques pour les agents OfficeScan à la page 14-55* pour plus d'informations.



AVERTISSEMENT!

Des paramètres proxy configurés par l'utilisateur incorrects peuvent entraîner des problèmes de mise à jour. Soyez prudent lorsque vous autorisez les utilisateurs à configurer leurs propres paramètres proxy.

Attribution de privilèges de configuration proxy

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Dans l'onglet **Privilèges**, accédez à la section **Privilèges de paramètres proxy**.
5. Sélectionnez **Autoriser les utilisateurs à configurer des paramètres proxy**.
6. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :
   - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.
   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Paramètres proxy automatiques pour les agents OfficeScan

La configuration manuelle des paramètres proxy peut s'avérer complexe pour la plupart des utilisateurs finaux. Utilisez la configuration automatique des paramètres proxy pour garantir l'application de paramètres proxy corrects sans que l'intervention de l'utilisateur soit requise.

Lorsqu'ils sont activés, les paramètres proxy automatiques sont prioritaires lorsque les agents OfficeScan mettent à jour les composants au moyen de la mise à jour automatique ou de l'option « Mettre à jour ». Voir *Méthodes de mise à jour des agents OfficeScan à la page 6-41* pour obtenir des informations complémentaires sur la mise à jour automatique et sur l'option Mettre à jour.

Si les agents OfficeScan ne peuvent pas se connecter à l'aide des paramètres proxy automatiques, les utilisateurs de ces agents bénéficiant du privilège de configuration des paramètres proxy peuvent procéder eux-mêmes à la configuration de ces paramètres. Sinon, la connexion à l'aide des paramètres proxy automatiques échoue.



Remarque

L'authentification du serveur proxy n'est pas prise en charge.

Configuration des paramètres proxy automatiques

Procédure

1. Accédez à **Agents** > **Paramètres généraux de l'agent**.
2. Allez dans la section **Configuration proxy**.
3. Sélectionnez **Détecter automatiquement les paramètres** si vous souhaitez qu'OfficeScan détecte automatiquement les paramètres proxy configurés par l'administrateur par DHCP ou DNS.
4. Si vous souhaitez qu'OfficeScan utilise le script de configuration proxy automatique (PAC, pour « proxy auto-configuration ») défini par l'administrateur réseau pour détecter le serveur proxy approprié :

a. Sélectionnez **Utiliser le script de configuration automatique**.

b. Tapez l'adresse du script PAC.

5. Cliquez sur **Enregistrer**.

Affichage des informations sur les agents OfficeScan

L'écran Afficher l'état affiche d'importantes informations relatives aux agents OfficeScan, notamment les privilèges, les informations détaillées sur le logiciel de l'agent et les événements système.

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **État**.
4. Affichez les informations relatives à l'état en développant le nom de l'endpoint de l'agent. Si vous avez sélectionné plusieurs agents, cliquez sur **Tout développer** pour afficher les informations relatives à l'état pour tous les agents sélectionnés.
5. (Facultatif) Utilisez le bouton **Réinitialiser** pour remettre à zéro le décompte de risques de sécurité.

Importation et exportation des paramètres d'un agent

OfficeScan vous permet d'exporter dans un fichier les paramètres de l'arborescence des agents appliqués par un agent ou un domaine OfficeScan particulier. Vous pouvez

ensuite importer ce fichier afin d'appliquer les paramètres à d'autres agents et domaines, ou vers un autre serveur OfficeScan d'une version identique.

Tous les paramètres de l'arborescence des agents, à l'exception des paramètres de l'agent de mise à jour, seront exportés.

Exportation des paramètres d'un agent

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Exporter paramètres**.
4. Cliquez sur l'un des liens pour afficher les paramètres de l'agent ou du domaine OfficeScan sélectionné.
5. Cliquez sur **Exporter** pour enregistrer les paramètres.

   Les paramètres sont enregistrés dans un fichier `.dat`.
6. Cliquez sur **Enregistrer**, puis indiquez dans quel dossier le fichier `.dat` doit être enregistré.
7. Cliquez sur **Enregistrer**.

Importation des paramètres d'un agent

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Importer des paramètres**.

4. Cliquez sur **Parcourir** pour localiser le fichier `.dat` sur le endpoint, puis cliquez sur **Importer**.

   L'écran **Importer les paramètres** apparaît ; il affiche un résumé des paramètres.

5. Cliquez sur un des liens pour afficher les informations concernant les paramètres de scan ou les privilèges à importer.

6. Procédez à l'importation des paramètres.

   - Si vous avez cliqué sur l'icône du domaine racine, sélectionnez **Appliquer à tous les domaines**, puis cliquez sur **Appliquer à la cible**.

   - Si vous avez sélectionné des domaines, sélectionnez **Appliquer à tous les ordinateurs appartenant au(x) domaine(s) sélectionné(s)**, puis cliquez sur **Appliquer à la cible**.

   - Si vous avez sélectionné plusieurs agents, cliquez sur **Appliquer à la cible**.

Conformité de la sécurité

Utilisez la conformité de la sécurité pour déterminer les failles, déployer des solutions et gérer l'infrastructure de sécurité. Cette fonctionnalité aide les administrateurs à réduire le temps requis pour sécuriser l'environnement réseau et permet d'équilibrer les besoins de l'entreprise en termes de sécurité et de fonctionnalité.

Appliquez la conformité de la sécurité pour deux types de endpoints :

- **Gérés** : endpoints sur lesquels se trouvent des agents OfficeScan gérés par le serveur OfficeScan. Pour obtenir des informations détaillées, voir *Conformité de la sécurité pour les agents gérés à la page 14-59*.

- **Non gérés** : Comprend les éléments suivants :

  - Agents OfficeScan non gérés par le serveur OfficeScan

  - Endpoints sur lesquels aucun agent OfficeScan n'est installé

  - Endpoints que le serveur OfficeScan ne peut atteindre

  - Endpoints dont l'état de sécurité ne peut être vérifié

Pour obtenir des informations détaillées, voir *Conformité de la sécurité pour les endpoints non gérés à la page 14-71*.

Conformité de la sécurité pour les agents gérés

La conformité de la sécurité génère un rapport de conformité pour vous aider à évaluer l'état de sécurité des agents OfficeScan gérés par le serveur OfficeScan. La conformité de la sécurité génère le rapport à la demande ou en fonction d'une programmation.

L'écran **Évaluation manuelle** affiche les onglets suivants :

- **Services** : utilisez cet onglet pour vérifier que les services des agents sont opérationnels. Pour obtenir des informations détaillées, voir *Services à la page 14-60*.
- **Composants** : utilisez cet onglet pour vérifier que les composants des agents OfficeScan sont à jour. Pour obtenir des informations détaillées, voir *Composants à la page 14-61*.
- **Conformité du scan** : utilisez cet onglet pour vérifier que les agents OfficeScan effectuent régulièrement des scans. Pour obtenir des informations détaillées, voir *Conformité du scan à la page 14-63*.
- **Paramètres** : utilisez cet onglet pour vérifier que les paramètres des agents sont cohérents avec ceux du serveur. Pour obtenir des informations détaillées, voir *Paramètres à la page 14-65*.



Remarque

L'onglet **Composants** peut afficher les agents OfficeScan utilisant la dernière version et les versions antérieures du produit. Pour les autres onglets, seuls les agents OfficeScan utilisant la version 10.5 ou 10.6 sont affichés.

Notes sur le rapport de conformité

- La conformité de la sécurité interroge l'état de connexion des agents OfficeScan avant de générer un rapport de conformité. Les agents en ligne et hors ligne sont inclus dans le rapport, mais pas les agents itinérants.
- Pour les comptes utilisateurs basés sur les rôles :

- Chaque compte utilisateur de la console Web possède un ensemble de paramètres de rapport de conformité totalement indépendant. Aucun changement dans les paramètres de rapport de conformité d'un compte utilisateur n'affectera les paramètres des autres comptes utilisateurs.
- L'étendue du rapport dépend des autorisations sur les domaines des agents des comptes utilisateurs. Par exemple, si vous accordez à un compte utilisateur les autorisations nécessaires pour gérer les domaines A et B, le rapport du compte utilisateur n'affichera que les données des agents appartenant aux domaines A et B.

  Pour obtenir des détails sur les comptes utilisateurs, voir *Administration basée sur les rôles à la page 13-2*.

Services

La conformité de la sécurité vérifie que les services des agents OfficeScan suivants sont opérationnels :

- Antivirus
- Anti-spyware
- Pare-feu
- Réputation de sites Web
- Surveillance des comportements/Contrôle des dispositifs (également désignés par Service de prévention des modifications non autorisées Trend Micro)
- Protection des données
- Connexion suspecte

Un agent non conforme est compté au minimum deux fois dans le rapport de conformité.



FIGURE 14-3. Rapport de conformité - onglet Services

- Dans la catégorie **Endpoints dont les services ne sont pas conformes**
- Dans la catégorie pour laquelle l'agent OfficeScan n'est pas conforme. Par exemple, si le service Antivirus de l'agent OfficeScan n'est pas opérationnel, l'agent est compté dans la catégorie **Antivirus**. Si plusieurs services ne sont pas opérationnels, l'agent est compté dans chaque catégorie pour laquelle il n'est pas conforme.

Redémarrez les services non opérationnels à partir de la console Web ou depuis l'agent OfficeScan. Si les services sont opérationnels après le redémarrage, l'agent n'apparaît plus comme non conforme lors de l'évaluation suivante.

Composants

La conformité de la sécurité détermine les incohérences de versions de composants entre le serveur OfficeScan et les agents OfficeScan. Ces incohérences se produisent généralement lorsque les agents ne peuvent pas se connecter au serveur pour mettre à

jour les composants. Si l'agent obtient des mises à jour d'une autre source (telle que le serveur ActiveUpdate de Trend Micro), il est possible que la version d'un composant d'un agent soit plus récente que celle du serveur.

La conformité de la sécurité vérifie les composants suivants :

- Smart Scan Agent Pattern
- Fichier de signatures de virus
- Signatures IntelliTrap
- Signatures d'exceptions IntelliTrap
- Moteur de scan antivirus
- Signatures de spywares
- Signatures de surveillance active des spywares
- Moteur de scan anti-spyware
- Modèle de nettoyage de virus
- Moteur de nettoyage de virus
- Signatures du pare-feu commun
- Pilote du pare-feu commun
- Pilote de surveillance des comportements
- Service principal de surveillance des comportements
- Modèle de configuration de la surveillance des comportements
- Digital Signature Pattern
- Modèle de conformité aux stratégies
- Signatures de détection de l'analyse comportementale
- Liste d'adresses IP C&C
- Fichier de signatures de règle de pertinence
- Early Boot Clean Driver
- Fichier de signatures de déclenchement du scan de la mémoire
- Fichier de signatures d'inspection de la mémoire
- Fichier de signatures de prévention contre l'exploitation du navigateur
- Fichier de signatures de l'analyseur de script
- Version du programme

Un agent non conforme est compté au minimum deux fois dans le rapport de conformité.



FIGURE 14-4. Rapport de conformité - onglet Composants

- Dans la catégorie **Ordinateurs disposant de versions des composants incohérentes**
- Dans la catégorie pour laquelle l'agent n'est pas conforme. Par exemple, si la version du fichier Smart Scan Agent Pattern de l'agent n'est pas cohérente avec la version du serveur, l'agent est compté dans la catégorie **Smart Scan Agent Pattern**. Si plusieurs versions de composants sont incohérentes, l'agent est compté dans chaque catégorie pour laquelle il n'est pas conforme.

Pour résoudre les incohérences des versions des composants, mettez à jour les composants obsolètes sur les agents ou sur le serveur.

Conformité du scan

La conformité de la sécurité vérifie si le scan immédiat ou le scan programmé sont exécutés régulièrement et s'ils sont effectués dans un délai raisonnable.



Remarque

La conformité de la sécurité ne peut rapporter l'état du scan programmé que si le scan programmé est activé sur les agents.

La conformité de la sécurité utilise les critères de conformité du scan suivants :

- **Aucun scan immédiat ou programmé n'a été effectué dans les (x) derniers jours** : un agent OfficeScan n'est pas conforme s'il n'a pas exécuté de scan immédiat ou de scan programmé depuis le nombre de jours spécifié.
- **Le scan immédiat ou programmé a dépassé (x) heures** : un agent OfficeScan n'est pas conforme si la durée du dernier scan immédiat ou programmé a dépassé le nombre d'heures spécifié.

Un agent non conforme est compté au minimum deux fois dans le rapport de conformité.

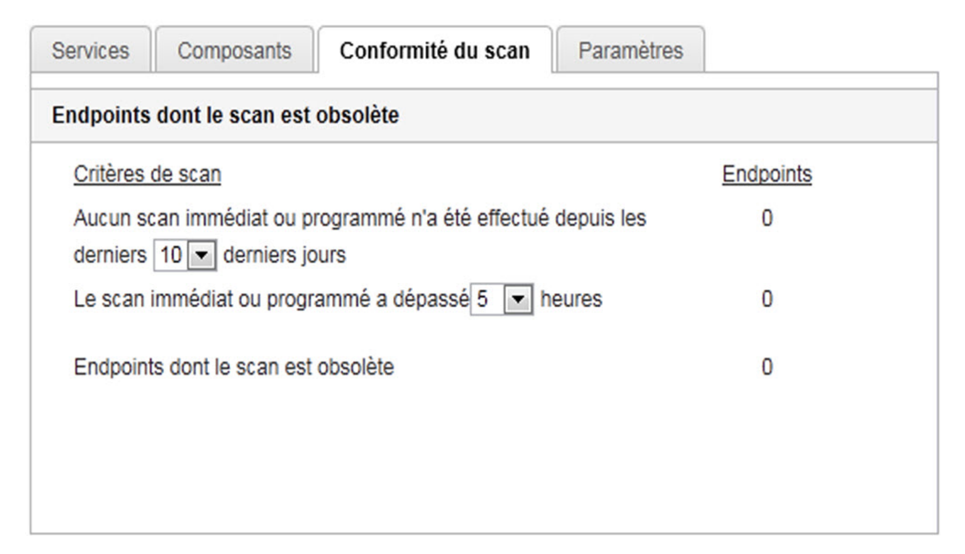


FIGURE 14-5. Rapport de conformité - onglet Conformité du scan

- Dans la catégorie **Endpoints dont le scan est obsolète**

- Dans la catégorie pour laquelle l'agent n'est pas conforme. Par exemple, si la durée du dernier scan programmé a dépassé le nombre d'heures spécifié, l'agent est compté dans la catégorie **Le scan immédiat ou programmé a dépassé <x> heures**. Si l'agent remplit plusieurs critères de conformité du scan, il est compté dans chaque catégorie pour laquelle il n'est pas conforme.

Exécutez le scan immédiat ou le scan programmé sur les agents qui n'ont pas effectué de tâches de scan ou n'ont pas pu terminer le scan.

Paramètres

La conformité de la sécurité détermine si les agents ont les mêmes paramètres que leurs domaines parents dans l'arborescence des agents. Les paramètres peuvent être incohérents si vous déplacez un agent vers un autre domaine qui applique un ensemble de paramètres différent ou si l'utilisateur d'un agent possédant certains privilèges a configuré manuellement des paramètres sur la console de l'agent OfficeScan.

OfficeScan vérifie les paramètres suivants :

- Méthode de scan
- Paramètres de scan manuel
- Paramètres de scan en temps réel
- Paramètres de scan programmé
- Paramètres de scan immédiat
- Privilèges et autres paramètres
- Paramètres des services complémentaires
- Réputation de sites Web
- Surveillance des comportements
- Contrôle des dispositifs
- Liste des spywares/graywares approuvés
- Paramètres de prévention contre la perte de données
- Connexion suspecte

Un agent non conforme est compté au minimum deux fois dans le rapport de conformité.

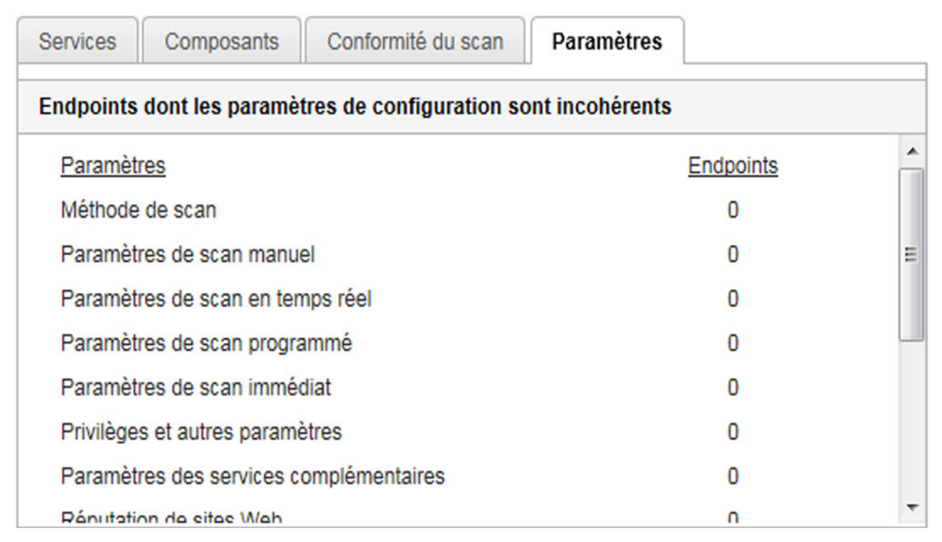


FIGURE 14-6. Rapport de conformité - onglet Paramètres

- Dans la catégorie **Endpoints dont les paramètres de configuration sont incohérents**
- Dans la catégorie pour laquelle l'agent n'est pas conforme. Par exemple, si les paramètres de méthode de scan d'un agent et de son domaine parent ne sont pas cohérents, l'agent est compté dans la catégorie **Méthode de scan**. Si plusieurs ensembles de paramètres sont incohérents, l'agent est compté dans chaque catégorie pour laquelle il n'est pas conforme.

Pour résoudre les incohérences de paramètres, appliquez à l'agent les paramètres du domaine.

Rapports de conformité à la demande

La conformité de la sécurité peut générer des rapports de conformité à la demande. Les rapports vous permettent d'évaluer l'état de sécurité des agents OfficeScan gérés par le serveur OfficeScan.

Pour plus d’informations sur les rapports de conformité, consultez la rubrique *Conformité de la sécurité pour les agents gérés à la page 14-59*.

Génération d'un rapport de conformité à la demande

Procédure

1. Accédez à **Évaluation** > **Conformité de la sécurité** > **Rapport manuel**.
2. Accédez à la section **Étendue de l'arborescence des agents**.
3. Sélectionnez un domaine ou le domaine racine et cliquez sur **Évaluer**.
4. Affichez le rapport de conformité pour les services de l'agent.

   Pour plus d'informations concernant les services de l'agent, voir *Services à la page 14-60*.

   a. Cliquez sur l'onglet **Services**.

   b. Sous **Endpoints dont les services ne sont pas conformes**, vérifiez le nombre d'agents dont les services ne sont pas conformes.

   c. Cliquez sur un lien chiffré pour afficher tous les agents concernés dans l'arborescence des agents.

   d. Sélectionnez les agents à partir des résultats de la requête.

   e. Cliquez sur **Redémarrer l'agent OfficeScan** pour redémarrer le service.



Remarque

Si, après avoir effectué une autre évaluation, l'agent apparaît encore comme non conforme, redémarrez manuellement le service sur le endpoint de l'agent.

f. Pour enregistrer la liste des agents dans un fichier, cliquez sur **Exporter**.

5. Affichez le rapport de conformité pour les composants de l'agent.

Pour plus d'informations sur les composants de l'agent, voir *Composants à la page 14-61*.

a. Cliquez sur l'onglet **Composants**.

b. Sous **Endpoints dont les versions des composants sont incohérentes**, vérifiez le nombre d'agents dont les versions des composants sont incohérentes avec celles du serveur.

c. Cliquez sur un lien chiffré pour afficher tous les agents concernés dans l'arborescence des agents.



Remarque

Si au moins l'un des agents possède un composant plus récent que le serveur OfficeScan, mettez le serveur OfficeScan à jour manuellement.

d. Sélectionnez les agents à partir des résultats de la requête.

e. Cliquez sur **Mettre à jour** pour forcer les agents à télécharger des composants.



Remarque

- Pour vous assurer que les agents peuvent mettre à niveau le programme de l'agent, désactivez l'option **Les agents OfficeScan peuvent mettre à jour les composants, mais ne peuvent pas mettre à niveau le programme de l'agent, ni déployer des correctifs de type hot fix** sous **Agents** > **Gestion des agents > Paramètres** > **Privilèges et autres paramètres**.
- Redémarrez le endpoint au lieu de cliquer sur **Mettre à jour** pour mettre à jour le pilote du pare-feu commun.

f. Pour enregistrer la liste des agents dans un fichier, cliquez sur **Exporter**.

6. Affichez le rapport de conformité pour les scans.

Pour plus de détails sur les scans, voir *Conformité du scan à la page 14-63*.

a. Cliquez sur l'onglet **Conformité du scan**.

b. Sous **Endpoints dont le scan est obsolète**, configurez les paramètres suivants :

- Nombre de jours pendant lesquels un agent n'a pas exécuté de scan immédiat ou de scan programmé
- Nombre d'heures depuis le début de l'exécution du scan immédiat ou programmé



Remarque

Si le nombre de jours ou d'heures est dépassé, l'agent est considéré comme non conforme.

c. Cliquez sur **Évaluer** en regard de la section **Étendue de l'arborescence des agents**.

d. Sous **Endpoints dont le scan est obsolète**, vérifiez le nombre d'agents répondant aux critères de scan.

e. Cliquez sur un lien chiffré pour afficher tous les agents concernés dans l'arborescence des agents.

f. Sélectionnez les agents à partir des résultats de la requête.

g. Cliquez sur **Scan immédiat** pour lancer un scan immédiat sur les agents.



Remarque

Pour éviter de recommencer le scan, l'option **Scan immédiat** sera désactivée si le scan immédiat a duré plus longtemps que le nombre d'heures spécifié.

h. Pour enregistrer la liste des agents dans un fichier, cliquez sur **Exporter**.

7. Affichez le rapport de conformité pour les paramètres.

Pour plus de détails sur les paramètres, voir *Paramètres à la page 14-65*.

a. Cliquez sur l'onglet **Paramètres**.

b. Sous **Ordinateurs dont les paramètres de configuration sont incohérents**, vérifiez le nombre d'agents dont les paramètres sont incohérents avec les paramètres de domaine de l'arborescence des agents.

c. Cliquez sur un lien chiffré pour afficher tous les agents concernés dans l'arborescence des agents.

d. Sélectionnez les agents à partir des résultats de la requête.

e. Cliquez sur **Appliquer les paramètres de domaine**.

f. Pour enregistrer la liste des agents dans un fichier, cliquez sur **Exporter**.

Rapports de conformité planifiés

La conformité de la sécurité peut générer des rapports de conformité en fonction d'un calendrier. Les rapports vous permettent d'évaluer l'état de sécurité des agents OfficeScan gérés par le serveur OfficeScan.

Pour plus d’informations sur les rapports de conformité, consultez la rubrique *Conformité de la sécurité pour les agents gérés à la page 14-59*.

Configuration des paramètres pour les rapports de conformité programmés

---

Procédure

1. Accédez à **Évaluation** > **Conformité de la sécurité** > **Rapport programmé**.
2. Sélectionnez **Activer la génération de rapports programmés**.
3. Spécifiez le titre du rapport.
4. Sélectionnez tout ou partie des options suivantes :
    - *Services à la page 14-60*
    - *Composants à la page 14-61*
    - *Conformité du scan à la page 14-63*

- *Paramètres à la page 14-65*

5. Spécifiez les adresses e-mail auxquelles seront envoyées les notifications concernant les rapports de conformité programmés.



Remarque

Configurez les paramètres de notification par courrier électronique pour vous assurer que les notifications par courrier électronique seront envoyées correctement. Pour obtenir des informations détaillées, voir *Paramètres de notification aux administrateurs à la page 13-33*.

6. Indiquez la programmation.

7. Cliquez sur **Enregistrer**.

Conformité de la sécurité pour les endpoints non gérés

La conformité de la sécurité peut interroger des endpoints non gérés dans le réseau auquel le serveur OfficeScan appartient. Utilisez Active Directory et les adresses IP pour interroger des endpoints.

L'état de sécurité des endpoints non gérés peut être l'un des suivants :

TABLEAU 14-8. État de sécurité des endpoints non gérés

ÉTAT	DESCRIPTION
Géré par un autre serveur OfficeScan	Les agents OfficeScan installés sur les ordinateurs sont gérés par un autre serveur OfficeScan. Les agents OfficeScan sont en ligne et exécutent cette version d'OfficeScan ou une version antérieure.
Aucun agent OfficeScan installé	L'agent OfficeScan n'est pas installé sur ce endpoint.
Non accessible	Le serveur OfficeScan ne parvient pas à se connecter au endpoint, ni à déterminer son état de sécurité.

ÉTAT	DESCRIPTION
Évaluation d'Active Directory non résolue	Le endpoint appartient à un domaine Active Directory, mais le serveur OfficeScan est incapable de déterminer son état de sécurité. **Remarque** La base de données du serveur OfficeScan contient une liste d'agents gérés par le serveur. Le serveur interroge Active Directory pour obtenir les GUID des ordinateurs et les compare ensuite à ceux enregistrés dans la base de données. Si un GUID ne figure pas dans la base de données, le endpoint sera rangé dans la catégorie Évaluation d'Active Directory non résolue.

Pour lancer une évaluation de la sécurité, effectuez les tâches suivantes :

1. Définissez l'étendue de la requête. Pour obtenir des informations détaillées, voir *Définition de l'étendue d'Active Directory/des adresses IP et de la requête. à la page 14-72*.

2. Vérifiez les ordinateurs non protégés à partir du résultat de la requête. Pour obtenir des informations détaillées, voir *Affichage des résultats de la requête à la page 14-75*.

3. Installez l'agent OfficeScan. Pour obtenir des informations détaillées, voir *Installation avec la conformité à la sécurité à la page 5-64*.

4. Configurez les requêtes programmées. Pour obtenir des informations détaillées, voir *Configuration l'évaluation de la requête programmée à la page 14-76*.

Définition de l'étendue d'Active Directory/des adresses IP et de la requête.

Lorsque vous effectuez une requête pour la première fois, définissez l'étendue d'Active Directory/des adresses IP, qui comprend les objets Active Directory et les adresses IP que le serveur OfficeScan interrogera à la demande ou périodiquement. Une fois l'étendue définie, lancez le processus d'interrogation.



Remarque

Pour définir une étendue Active Directory, Office Scan doit d'abord être intégré à Active Directory. Pour plus de détails sur l'intégration, voir *Intégration d'Active Directory à la page 2-36*.

Procédure

1. Accédez à **Évaluation** > **Endpoints non gérés**.
2. Dans la section **Étendue Active Directory/adresse IP**, cliquez sur **Définir**. Un nouvel écran s'affiche.
3. Pour définir une étendue d'Active Directory :
   a. Accédez à la section **Étendue Active Directory**.
   b. Sélectionnez **Utiliser les évaluations à la demande** afin d'effectuer des requêtes en temps réel et de parvenir à des résultats plus précis. Lorsque cette option est désactivée, OfficeScan interroge la base de données, et non chaque agent OfficeScan. Interroger uniquement la base de données s'avère plus rapide, mais également moins précis.
   c. Sélectionnez les objets à interroger. Si vous effectuez la requête pour la première fois, sélectionnez un objet comportant moins de 1,000 comptes et notez le temps nécessaire à l'exécution de la requête. Utilisez ces données comme point de référence pour les performances.
4. Pour définir une étendue des adresses IP :
   a. Accédez à la section **Étendue d'adresses IP**.
   b. Sélectionnez **Activer Étendue d'adresses IP**.
   c. Spécifiez une plage d'adresses IP. Cliquez sur le bouton plus ou moins pour ajouter ou supprimer des plages d'adresses IP.
   - Pour un serveur OfficeScan IPv4 pur, saisissez une plage d'adresses IPv4.
   - Pour un serveur OfficeScan IPv6 pur, saisissez un préfixe et une longueur IPv6.

- Pour un serveur OfficeScan double pile, saisissez une plage d'adresses IPv4 et/ou un préfixe et une longueur IPv6.

  La plage d'adresses IPv6 est limitée à 16 bits, ce qui est similaire aux plages d'adresses IPv4. La longueur du préfixe doit ainsi être comprise entre 112 et 128.

TABLEAU 14-9. Longueurs de préfixe et nombre d'adresses IPv6

LONGUEUR	NOMBRE D'ADRESSES IPV6
128	2
124	16
120	256
116	4,096
112	65,536

5. Sous Paramètre avancés, spécifiez les ports utilisés par les serveurs OfficeScan pour communiquer avec les agents. Le programme d'installation génère de manière aléatoire le numéro de port pendant l'installation du serveur OfficeScan.

Pour afficher le port de communication utilisé par le serveur OfficeScan, accédez à **Agents** > **Gestion des agents** et sélectionnez un domaine. Le port s'affiche en regard de la colonne d'adresse IP. Trend Micro vous recommande de noter les numéros de port à titre de référence.

a. Cliquez sur **Spécifier les ports**.

b. Saisissez le numéro de port et cliquez sur **Ajouter**. Reprenez cette opération jusqu'à ce que tous les numéros de port que vous souhaitez ajouter s'affichent.

c. Cliquez sur **Enregistrer**.

6. Pour vérifier la connectivité d'un endpoint en utilisant un numéro de port particulier, sélectionnez **Déclarer un endpoint inaccessible en vérifiant le port <x>**. Si la connexion n'est pas établie, OfficeScan considère immédiatement que le endpoint est inaccessible. Le numéro de port par défaut est 135.

L'activation de ce paramètre accélère la requête. Lorsqu'il ne parvient pas à établir la communication avec un endpoint, le serveur OfficeScan n'a plus besoin

d'effectuer toutes les autres tâches de vérification de la connexion avant de considérer un endpoint comme inaccessible.

7. Pour enregistrer l'étendue et lancer la requête, cliquez **Enregistrer et réévaluer**. Pour enregistrer uniquement les paramètres, cliquez sur **Enregistrer uniquement**. L'écran Gestion des serveurs externes affiche le résultat de la requête.



Remarque

La requête risque de prendre un certain temps, notamment si son étendue est importante. Ne lancez pas une autre requête tant que l'écran Gestion des serveurs externes n'affiche pas les résultats. Autrement, la session de requête actuelle prendra fin et le processus de requête redémarrera.

Affichage des résultats de la requête

Le résultat de la requête apparaît sous la section **État de sécurité**. Un endpoint non géré aura l'un des états suivants :

- Géré par un autre serveur OfficeScan
- Aucun agent OfficeScan installé
- Non accessible
- Évaluation d'Active Directory non résolue

Procédure

1. Dans la section **État de sécurité**, cliquez sur un lien numérique pour afficher tous les ordinateurs affectés.

2. Utilisez les fonctions de recherche et de recherche avancée pour rechercher et afficher uniquement les ordinateurs qui répondent aux critères de recherche.

   Si vous utilisez la fonction de recherche avancée, spécifiez les éléments suivants :

   - Plage d'adresses IPv4
   - Préfixe et longueur IPv6 (le préfixe doit être compris entre 112 et 128)

- Nom de l'Endpoint
- Nom du serveur OfficeScan
- Arborescence Active Directory
- État de sécurité

OfficeScan ne renvoie pas de résultat si le nom est incomplet. Vous pouvez utiliser un caractère générique (*) en cas de doute sur le nom complet.

3. Pour enregistrer la liste d'ordinateurs dans un fichier, cliquez sur **Exporter**.

4. Pour les agents OfficeScan gérés par un autre serveur OfficeScan, utilisez l'outil Agent Mover pour que ces agents OfficeScan soient gérés par le serveur OfficeScan actuel. Voir *Agent Mover à la page 14-23* pour obtenir des informations complémentaires sur cet outil.

Configuration l'évaluation de la requête programmée

Configurez le serveur OfficeScan pour interroger périodiquement Active Directory et les adresses IP afin de garantir que les stratégies de sécurité sont appliquées.

Procédure

1. Accédez à **Évaluation** > **Endpoints non gérés**.
2. Cliquez sur **Paramètres** en haut de l'arborescence des agents.
3. Activez la fonction de requête programmée.
4. Indiquez la programmation.
5. Cliquez sur **Enregistrer**.

Trend Micro Virtual Desktop Support

Optimisez la protection des bureaux virtuels en utilisant Trend Micro Virtual Desktop Support. Cette fonctionnalité régule les tâches sur les agents OfficeScan qui résident sur un serveur virtuel unique.

L'exploitation de plusieurs bureaux sur un seul serveur et l'exécution de scans à la demande ou de mises à jour de composants consomment une quantité importante de ressources système. Utilisez cette fonctionnalité pour empêcher les agents d'exécuter simultanément des scans ou des mises à jour de composants.

Par exemple, si un serveur VMware vCenter possède trois bureaux virtuels exécutant des agents OfficeScan, OfficeScan peut déclencher un scan immédiat et déployer simultanément des mises à jour sur les trois agents. Virtual Desktop Support détecte la présence des agents sur le même serveur physique. Virtual Desktop Support autorise le déroulement d'une tâche sur le premier agent et en retarde l'exécution sur les deux autres tant que la tâche n'est pas terminée sur le premier.

Virtual Desktop Support peut être utilisé sur les plates-formes suivantes :

- VMware vCenter™ (VMware View™)
- Citrix™ XenServer™ (Citrix XenDesktop™)
- Microsoft Hyper-V™ Server

Pour les administrateurs utilisant d'autres applications de virtualisation, le serveur OfficeScan peut également agir en tant que hyperviseur émulé pour gérer les agents virtuels.

Pour plus d'informations sur ces plates-formes, consultez les sites Web VMware View, Citrix XenDesktop ou Microsoft Hyper-V.

Utilisez l'outil OfficeScan de génération de modèle de pré-scan VDI pour optimiser les scans à la demande ou supprimer des GUID des images de base ou Golden.

Installation de Virtual Desktop Support

Virtual Desktop Support est une fonctionnalité native d'OfficeScan, mais nécessite une licence séparée. Après avoir installé le serveur OfficeScan, cette fonctionnalité est

disponible, mais pas opérationnelle. L'installation de cette fonctionnalité implique le téléchargement d'un fichier depuis le serveur ActiveUpdate (ou depuis une source de mise à jour personnalisée, si définie). Une fois le fichier intégré au serveur OfficeScan, vous pouvez activer Virtual Desktop Support pour que cette fonctionnalité soit totalement opérationnelle. L'installation et l'activation sont effectuées depuis Plug-in Manager.



Remarque

Virtual Desktop Support n'est pas complètement pris en charge dans les environnements en IPv6 pur. Pour obtenir des informations détaillées, voir *Limitations des serveurs IPv6 purs à la page A-3*.

Installation de Virtual Desktop Support

Procédure

1. Ouvrez la console Web OfficeScan, puis cliquez sur **Modules additionnels** dans le menu principal.

2. Dans l'écran **Plug-in Manager**, accédez à la section **Trend Micro Virtual Desktop Support** et cliquez sur **Télécharger**.

   La taille du pack s'affiche en regard du bouton **Télécharger**.

   Plug-In Manager stocke le package téléchargé dans le répertoire <*dossier d'installation du serveur*>`\PCCSRV\Download\Product`.

   Remarque

   Si Plug-in Manager ne peut pas télécharger le fichier, il relance automatiquement le téléchargement après 24 heures. Pour lancer manuellement le téléchargement du package par Plug-in Manager, redémarrez le service OfficeScan Plug-in Manager depuis Microsoft Management Console.

3. Surveillez la progression du téléchargement. Vous pouvez naviguer dans une autre fenêtre pendant le téléchargement.

Si vous rencontrez des problèmes lors du téléchargement du pack, consultez les journaux de mise à jour du serveur sur la console du produit OfficeScan. Dans le menu principal, cliquez sur **Journaux** > **Mise à jour du serveur**.

Une fois le fichier téléchargé par Plug-in Manager, Virtual Desktop Support s'affiche dans un nouvel écran.



Remarque

Si Virtual Desktop Support ne s'affiche pas, consultez les causes et les solutions dans *Dépannage de Plug-in Manager à la page 15-12*.

4. Pour installer Virtual Desktop Support immédiatement, cliquez sur **Installer**. Pour installer ultérieurement :

    a. Cliquez sur **Installer ultérieurement**.

    b. Ouvrez la fenêtre **Plug-in Manager**.

    c. Accédez à la section **Trend Micro Virtual Desktop Support**, puis cliquez sur **Installer**.

5. Lisez attentivement le contrat de licence, puis acceptez ses termes en cliquant sur **Accepter**.

    L'installation démarre.

6. Surveillez la progression de l'installation. Après l'installation, la version de Virtual Desktop Support s'affiche.

Licence de Virtual Desktop Support

Affichez, activez et renouvelez la licence de Virtual Desktop Support à partir du Plug-In Manager.

Obtenez le code d'activation auprès de Trend Micro, puis utilisez-le pour activer les fonctionnalités complètes de Virtual Desktop Support.

Activation ou renouvellement de Virtual Desktop Support

Procédure

1. Ouvrez la console Web OfficeScan, puis cliquez sur **Modules additionnels** dans le menu principal.
2. Sur l'écran **Plug-in Manager**, accédez à la section **Trend Micro Virtual Desktop Support** et cliquez sur **Manage Program**.
3. Cliquez sur **Afficher les informations de licence**.
4. Sur l'écran qui s'affiche, **Détails sur la licence du produit** cliquez sur **Nouveau code d'activation**.
5. Sur l'écran qui s'affiche, saisissez le code d'activation puis cliquez sur **Enregistrer**.
6. Lorsque vous revenez à l'écran Détails sur la licence du produit, cliquez sur **Informations sur la mise à jour** pour actualiser l'écran avec les nouvelles informations sur la licence et l'état de la fonction. Cet écran fournit également un lien vers le site Web de Trend Micro sur lequel vous trouverez des informations détaillées relatives à votre licence.

Affichage des informations relatives à la licence de Virtual Desktop Support

Procédure

1. Ouvrez la console Web OfficeScan, puis cliquez sur **Modules additionnels** > **[Trend Micro Virtual Desktop Support] Gestion de programme** dans le menu principal.
2. Cliquez sur **Afficher les informations de licence**.
3. Consultez les informations relatives à la licence dans l'écran qui s'ouvre.

   La section Détails de la licence de Virtual Desktop Support fournit les informations suivantes :

   - **État** : affiche « Activé », « Non activé » ou « Expiré ».

- **Version** : affiche la version « complète » ou d'« évaluation ». Si vous disposez à la fois de la version complète et de versions d'évaluation, la version qui s'affiche alors est la version « complète ».
- **Date d'expiration** : Si Virtual Desktop Support dispose de plusieurs licences, la dernière date d'expiration s'affiche. Par exemple, si les dates d'expiration de la licence sont le 31/12/2010 et le 30/06/2010, la date qui s'affiche est le 31/12/2010.
- **Postes** : Affiche le nombre d'agents OfficeScan pouvant utiliser Virtual Desktop Support
- **Code d'activation** : affiche le code d'activation

Des messages de rappel concernant les licences s'affichent dans les cas suivants:

Si vous possédez une licence de version complète :

- Pendant la période de grâce de la fonction. La durée de la période de grâce varie selon les régions. Veuillez vérifier cette durée auprès de votre représentant Trend Micro.
- Une fois la licence expirée et la période de grâce écoulée: pendant cette période, vous ne pourrez pas obtenir d'assistance technique.

Si vous possédez une licence de version d'évaluation

- Une fois la licence expirée: pendant cette période, vous ne pourrez pas obtenir d'assistance technique.

4. Cliquez sur **Afficher le détail de la licence en ligne** pour afficher les informations relatives à votre licence sur le site Web de Trend Micro.
5. Pour rafraîchir l'écran avec les dernières informations de licence, cliquez sur **Informations sur la mise à jour**.

Connexions Virtual Server

Optimisez les scans à la demande ou les mises à jour de composants en ajoutant VMware vCenter 4 (VMware View 4), Citrix XenServer 5.5 (Citrix XenDesktop 4) ou Microsoft Hyper-V Server. Les serveurs OfficeScan communiquent avec les serveurs

virtuels indiqués pour identifier les agents OfficeScan qui résident sur le même serveur physique.

Pour les autres serveurs VDI, le serveur OfficeScan fournit un hyperviseur virtuel émulé pour gérer les agents virtuels sur d'autres plates-formes. L'hyperviseur OfficeScan traite les requêtes des agents virtuels dans l'ordre dans lequel le serveur les reçoit. Le serveur OfficeScan traite une requête à la fois et place les autres dans une file d'attente.

Ajout de connexions serveur

Procédure

1. Ouvrez la console Web OfficeScan, puis cliquez sur **Modules additionnels** > **[Trend Micro Virtual Desktop Support] Gestion de programme** dans le menu principal.

2. Sélectionnez **Serveur VMware vCenter**, **Citrix XenServer**, **Microsoft Hyper-V** ou **Autres applications de virtualisation**.



Remarque

Si vous sélectionnez **Autres applications de virtualisation**, aucune information supplémentaire n'est à fournir. Le serveur OfficeScan répond aux requêtes des agents virtuels dans l'ordre dans lequel il les reçoit.

3. Activez la connexion au serveur.

4. Indiquez les informations suivantes :

    - Pour les serveurs VMware vCenter et Citrix XenServer :

        - adresse IP
        - Port
        - Protocole de connexion (HTTP ou HTTPS)
        - Nom d'utilisateur
        - Mot de passe

    - Pour les serveurs Microsoft Hyper-V :

- Nom ou adresse IP de l'hôte
- Domaine\Nom d'utilisateur



Remarque

Le compte de connexion doit être un compte de domaine dans le groupe Administrateurs

- Mot de passe

5. Activez éventuellement la connexion proxy pour VMware vCenter ou Citrix XenServer.

   a. Indiquez le nom ou l'adresse IP et le numéro de port du serveur proxy.

   b. Si le serveur proxy nécessite une authentification, indiquez le nom d'utilisateur et le mot de passe appropriés.

6. Cliquez sur **Tester la connexion** pour vérifier que le serveur OfficeScan se connecte correctement au serveur.



Remarque

Pour plus d'informations sur les connexions Microsoft Hyper-V, consultez *Dépannage des connexions Microsoft Hyper-V à la page 14-86*.

7. Cliquez sur **Enregistrer**.

Ajout de plusieurs connexions serveur

Procédure

1. Ouvrez la console Web OfficeScan, puis cliquez sur **Modules additionnels** > **[Trend Micro Virtual Desktop Support] Gestion de programme** dans le menu principal.

2. Cliquez sur **Ajouter une connexion vCenter**, **Ajouter une connexion XenServer** ou sur **Ajouter une connexion Hyper-V**.

3. Reprenez la procédure permettant de fournir les informations de serveur appropriées.

4. Cliquez sur **Enregistrer**.

Suppression d'un paramètre de connexion

Procédure

1. Ouvrez la console Web OfficeScan, puis accédez à **Modules additionnels** > **[Trend Micro Virtual Desktop Support] Gestion de programme** dans le menu principal.

2. Cliquez sur **Supprimer cette connexion**.

3. Cliquez sur **Ok** pour confirmer la suppression de ce paramètre.

4. Cliquez sur **Enregistrer**.

Modification de la capacité de scan VDI

Les administrateurs peuvent augmenter le nombre de endpoints VDI exécutant des scans simultanés en modifiant le fichier `vdi.ini`. Trend Micro recommande de surveiller de très près les effets de la modification de la capacité VDI afin de s'assurer que les ressources système peuvent prendre en charge une telle augmentation du volume de scan.

Procédure

1. Sur l'ordinateur du serveur OfficeScan, accédez au fichier <*dossier d'installation du serveur*>`PCCSRV\Private\vdi.ini`.

2. Localisez le paramètre `[TaskController]`.

   Les paramètres TaskController par défaut sont les suivants :

   - Pour les clients OfficeScan 10.5 :

```
[TaskController]
Controller_00_MaxConcurrentGuests=1
Controller_01_MaxConcurrentGuests=3
```

Où :

- `Controller_00_MaxConcurrentGuests=1` équivaut au nombre maximal de clients pouvant effectuer des scans simultanément.
- `Controller_01_MaxConcurrentGuests=3` équivaut au nombre maximal de clients pouvant effectuer des mises à jour simultanément.

- Pour les clients OfficeScan 10.6 et les agents OfficeScan 11.0 :

```
[TaskController]
Controller_02_MaxConcurrentGuests=1
Controller_03_MaxConcurrentGuests=3
```

Où :

- `Controller_02_MaxConcurrentGuests=1` équivaut au nombre maximal de clients pouvant effectuer des scans simultanément.
- `Controller_03_MaxConcurrentGuests=3` équivaut au nombre maximal de clients pouvant effectuer des mises à jour simultanément.

3. Augmentez ou diminuez la valeur de chaque contrôleur selon vos besoins.

La valeur minimale pour tous les paramètres est 1.

La valeur maximale pour tous les paramètres est 65536.

4. Enregistrez et fermez le fichier `vdi.ini`.

5. Redémarrez le service principal d'OfficeScan.

6. Surveillez les ressources (processeur, mémoire et disque) des endpoints VDI. Répétez les étapes 1 à 5 afin d'augmenter ou de diminuer à nouveau le nombre de

scans simultanés de façon à ce que les paramètres du contrôleur correspondent au mieux à votre environnement VDI.

Dépannage des connexions Microsoft Hyper-V

La connexion Microsoft Hyper-V utilise WMI (Windows Management Instrumentation) et DCOM pour la communication agent-serveur. Les stratégies de pare-feu peuvent bloquer cette communication, entraînant ainsi l'échec de la connexion au serveur Hyper-V.

Le port d'écoute du serveur Hyper-V est, par défaut, défini sur le port 135 et sélectionne de façon aléatoire un port configuré pour une communication ultérieure. Si le pare-feu bloque le trafic WMI ou l'un de ces deux ports, la communication avec le serveur échoue. Les administrateurs peuvent modifier la stratégie du pare-feu pour permettre une bonne communication avec le serveur Hyper-V.

Vérifiez que tous les paramètres de connexion, notamment l'adresse IP, le domaine, le nom d'utilisateur et le mot de passe sont corrects avant d'effectuer les modifications du pare-feu suivantes.

Permettre la communication WMI via le pare-feu Windows

Procédure

1. Sur le serveur Hyper-V, ouvrez la fenêtre **Programmes autorisés du pare-feu Windows**.

   Sur les systèmes Windows 2008 R2, accédez à **panneau de configuration** > **système et sécurité** > **pare-feu Windows** > **autorise un programme ou une fonction via le pare-feu Windows**.

2. Sélectionnez **Windows Management Instrumentation (WMI)**.

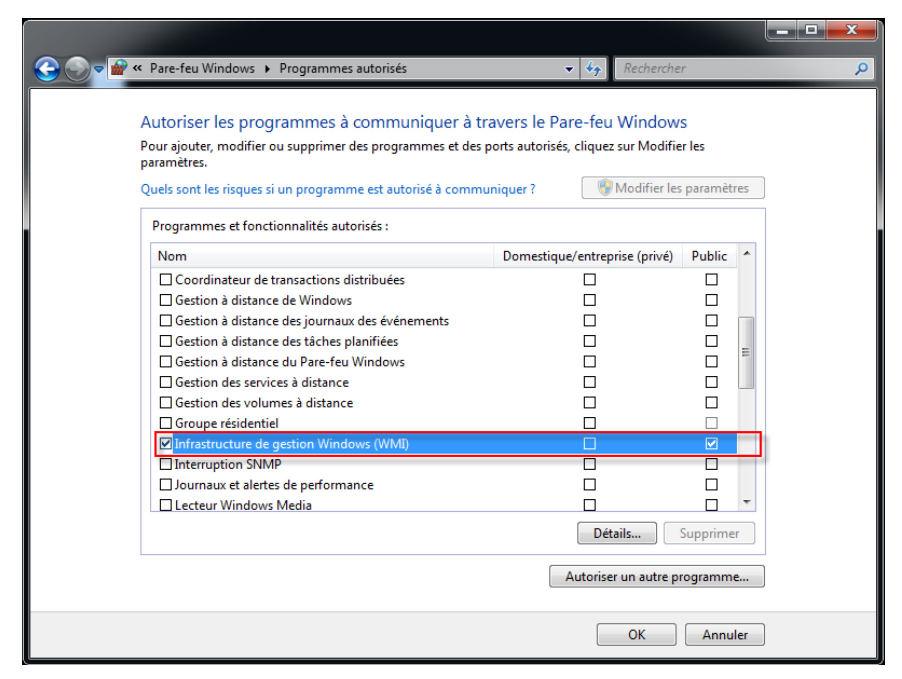


FIGURE 14-7. Programme d'écran autorisé du pare-feu Windows

3. Cliquez sur **Enregistrer**.

4. Testez à nouveau la connexion Hyper-V.

Ouverture du port de communication via le pare-feu Windows ou un pare-feu tiers

Procédure

1. Sur le serveur Hyper-V, assurez-vous que le pare-feu permet la communication via le port 135 puis testez la connexion Hyper-V à nouveau.

   Pour des informations supplémentaires concernant l'ouverture des ports, reportez-vous à votre documentation de pare-feu.

2. Si la connexion au serveur Hyper-V échoue, configurez WMI pour utiliser un port fixe.

   Pour plus d'informations concernant *configuration d'un port fixe pour WMI*, reportez-vous à :

   http://msdn.microsoft.com/en-us/library/windows/desktop/bb219447(v=vs.85).aspx

3. Ouvrez les ports 135 et le port fixe nouvellement créé (24158) pour une communication via le pare-feu.

4. Testez à nouveau la connexion Hyper-V.

Outil de génération de modèle de pré-scan VDI

Utilisez l'outil de génération de modèle de pré-scan VDI OfficeScan pour optimiser les scans à la demande ou supprimer des GUID d'images de base ou Golden. Cet outil scanne l'image de base ou Golden et la certifie. Lorsque le scan duplique l'image, OfficeScan vérifie uniquement les parties qui ont été modifiées. Le délai de scan est ainsi réduit.



Conseil

Trend Micro recommande de générer le modèle de pré-scan après une mise à jour Windows ou après l'installation d'une nouvelle application.

Création d'un modèle de pré-scan

Procédure

1. Sur l'ordinateur du serveur OfficeScan, accédez au répertoire <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\TCacheGen`.

2. Choisissez une version de l'outil de génération de modèle de pré-scan VDI. Les versions suivantes sont à votre disposition :

TABLEAU 14-10. Versions de l'outil de génération de modèle de pré-scan VDI

NOM DU FICHIER	INSTRUCTION
TCacheGen.exe	Sélectionnez ce fichier si vous souhaitez exécuter l'outil directement sur une plate-forme 32 bits.
TCacheGen_x64.exe	Sélectionnez ce fichier si vous souhaitez exécuter l'outil directement sur une plate-forme 64 bits.
TCacheGenCli.exe	Sélectionnez ce fichier si vous souhaitez exécuter l'outil depuis l'interface de ligne de commande d'une plate-forme 32 bits.
TCacheGenCli_x64.exe	Sélectionnez ce fichier si vous souhaitez exécuter l'outil depuis l'interface de ligne de commande d'une plate-forme 64 bits.

3. Copiez sur le endpoint la version de l'outil que vous avez choisi à l'étape précédente.

4. Exécutez l'outil.

- Pour exécuter l'outil directement :

  a. Double-cliquez sur `TCacheGen.exe` ou `TCacheGen_x64.exe`.

  b. Sélectionnez **Générer un modèle de pré-scan** et cliquez sur **Suivant**.

- Pour exécuter l'outil depuis l'interface de ligne de commande :

  a. Ouvrez une invite de commandes et remplacez le répertoire existant par le `<dossier d'installation de l'agent>`.

  b. Saisissez la commande suivante :

  ```
  TCacheGenCli Generate_Template
  ```

  Ou

  ```
  TcacheGenCli_x64 Generate_Template
  ```



Remarque

Avant de générer le modèle de pré-scan et de supprimer le GUID, l'outil scanne l'image pour détecter d'éventuelles menaces de sécurité.

Une fois le modèle de pré-scan généré, l'outil décharge l'agent OfficeScan. Ne rechargez pas l'agent OfficeScan. Si celui-ci se recharge, vous devrez recréer le modèle de pré-scan.

Suppression de GUID des modèles

Procédure

1. Sur l'ordinateur du serveur OfficeScan, accédez au répertoire <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\TCacheGen`.

2. Choisissez une version de l'outil de génération de modèle de pré-scan VDI. Les versions suivantes sont à votre disposition :

TABLEAU 14-11. Versions de l'outil de génération de modèle de pré-scan VDI

NOM DU FICHIER	INSTRUCTION
TCacheGen.exe	Sélectionnez ce fichier si vous souhaitez exécuter l'outil directement sur une plate-forme 32 bits.
TCacheGen_x64.exe	Sélectionnez ce fichier si vous souhaitez exécuter l'outil directement sur une plate-forme 64 bits.
TCacheGenCli.exe	Sélectionnez ce fichier si vous souhaitez exécuter l'outil depuis l'interface de ligne de commande d'une plate-forme 32 bits.
TCacheGenCli_x64.exe	Sélectionnez ce fichier si vous souhaitez exécuter l'outil depuis l'interface de ligne de commande d'une plate-forme 64 bits.

3. Copiez sur le endpoint la version de l'outil que vous avez choisi à l'étape précédente.

4. Exécutez l'outil.

    - Pour exécuter l'outil directement :

a. Double-cliquez sur `TCacheGen.exe` ou `TCacheGen_x64.exe`.

b. Sélectionnez **Supprimer le GUID du modèle** et cliquez sur **Suivant**.

- Pour exécuter l'outil depuis l'interface de ligne de commande :

a. Ouvrez une invite de commandes et remplacez le répertoire existant par le `<dossier d'installation de l'agent>`.

b. Saisissez la commande suivante :

```
TCacheGenCli Remove GUID
```

Ou

```
TcacheGenCli_x64 Remove GUID
```

Paramètres généraux de l'agent

OfficeScan applique des paramètres généraux à tous les agents ou seulement aux agents disposant de certains privilèges.

Procédure

1. Accédez à **Agents** > **Paramètres généraux de l'agent**.
2. Configurez les paramètres suivants :

Tableau 14-12. Paramètres généraux de l'agent

Paramètre	Référence
Paramètres de scan	*Paramètres de scan généraux à la page 7-71*
Paramètres de scan programmé	*Paramètres de scan généraux à la page 7-71*

Paramètre	Référence
Paramètres de bande passante des journaux de virus/programmes malveillants	*Paramètres de scan généraux à la page 7-71*
Paramètres du pare-feu	*Paramètres généraux du pare-feu à la page 12-26*
Paramètres de surveillance des comportements	*Surveillance des comportements à la page 8-2*
Paramètres de Certified Safe Software Service	*Activer Certified Safe Software Service pour la surveillance des comportements, le pare-feu et les scans antivirus à la page 7-83*
Paramètres de connexion suspecte	*Configuration des paramètres des listes globales des adresses IP définies par l'utilisateur à la page 11-14*
Mises à jour	*Serveur ActiveUpdate en tant que source de mise à jour des agents OfficeScan à la page 6-41*
Espace disque réservé	*Configuration de l'espace disque réservé pour les mises à jour des agents OfficeScan à la page 6-53*
Réseau inaccessible	*Agents inaccessibles à la page 14-46*
Paramètres d'alerte	*Configuration des notifications de mise à jour des agents OfficeScan à la page 6-55*
Redémarrage du service d'OfficeScan	*Redémarrage des services de l'agent OfficeScan à la page 14-12*
Configuration proxy	*Paramètres proxy automatiques pour les agents OfficeScan à la page 14-55*
Adresse IP de votre choix	*Adresses IP des agents à la page 5-9*

3. Cliquez sur **Enregistrer**.

Configuration des privilèges des agents et d'autres paramètres

Accordez aux utilisateurs les privilèges de modification de certains paramètres et de réalisation des tâches de haut niveau sur l'agent OfficeScan.



Remarque

Les paramètres antivirus n'apparaissent uniquement qu'après activation de la fonctionnalité antivirus OfficeScan.



Conseil

Pour garantir l'uniformité des paramètres et des stratégies dans l'ensemble de l'entreprise, accordez aux utilisateurs des privilèges limités.

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.
4. Dans l'onglet **Privilèges**, configurez les privilèges utilisateur suivants :

Tableau 14-13. Privilèges sur l'agent

Privilèges sur l'agent	Référence
Privilège de mode itinérance	*Privilège des agents OfficeScan itinérants à la page 14-21*
Privilèges de scan	*Privilèges de type de scan à la page 7-56*
Privilèges de scan programmé	*Privilèges et autres paramètres de scan programmé à la page 7-59*
Privilèges du pare-feu	*Privilèges du pare-feu à la page 12-24*

Privilèges sur l'agent	Référence
Privilèges de surveillance des comportements	*Privilèges de surveillance des comportements à la page 8-12*
Privilèges du scan de courrier	*Privilèges et autres paramètres du scan de courrier à la page 7-65*
Privilèges de paramètres proxy	*Privilèges de configuration proxy pour les agents à la page 14-53*
Privilèges de mise à jour des composants	*Configuration des privilèges de mise à jour et d'autres paramètres à la page 6-51*
Déchargement et déverrouillage	*Affectation du privilège de déchargement et de déverrouillage de l'agent à la page 14-20*
Désinstallation	*Affectation du privilège de désinstallation de l'agent OfficeScan à la page 5-75*

5. Cliquez sur l'onglet **Autres paramètres**, puis configurez les paramètres suivants:

Tableau 14-14. Autres paramètres de l'agent

Paramètre	Référence
Paramètres de mise à jour	*Configuration des privilèges de mise à jour et d'autres paramètres à la page 6-51*
Paramètres de réputation de sites Web	*Notifications sur les menaces Internet pour les utilisateurs des agents à la page 11-17*
Paramètres de surveillance des comportements	*Privilèges de surveillance des comportements à la page 8-12*
Paramètres d'alerte de contact C&C	*Notifications des alertes de contact C&C pour les utilisateurs des agents à la page 11-22*
Paramètres d'alerte de restauration depuis la mise en quarantaine centrale	Affiche un message de notification sur le endpoint après la restauration d'un fichier mis en quarantaine
Autoprotection de l'agent OfficeScan	*Autoprotection de l'agent OfficeScan à la page 14-13*

PARAMÈTRE	RÉFÉRENCE
Paramètres de scan programmé	*Attribution de privilèges de scan programmé et affichage de la notification de privilège à la page 7-60*
Paramètres du cache pour les scans	*Paramètres du cache pour les scans à la page 7-67*
Paramètres de sécurité de l'agent OfficeScan	*Sécurité de l'agent OfficeScan à la page 14-17*
Paramètres de scan de la messagerie POP3	*Attribution des privilèges du scan de courrier et activation du scan de la messagerie POP3 à la page 7-66*
Restriction de l'accès à l'agent OfficeScan	*Restriction de l'accès à la console de l'agent OfficeScan à la page 14-18*
Notification de redémarrage	*Notifications sur les risques de sécurité pour les utilisateurs des agents OfficeScan à la page 7-88*

6. Si vous avez sélectionné un ou plusieurs domaines ou agents dans l'arborescence des agents, cliquez sur **Enregistrer**. Si vous avez cliqué sur l'icône de domaine racine, choisissez parmi les options suivantes :

   - **Appliquer à tous les agents** : applique les paramètres à tous les agents existants et à tout nouvel agent ajouté à un domaine existant/futur. Les domaines futurs sont des domaines qui n'ont pas encore été créés lors de la configuration des paramètres.

   - **Appliquer aux domaines futurs uniquement** : applique les paramètres uniquement aux agents ajoutés aux domaines futurs. Cette option ne permet pas d'appliquer les paramètres aux nouveaux agents ajoutés à un domaine existant.

Partie IV

Protection supplémentaire



Chapitre 15

Utilisation de Plug-in Manager

Ce chapitre aborde la configuration de Plug-in Manager et présente les solutions modules additionnels fournies via Plug-in Manager.

Les rubriques sont les suivantes :

À propos de Plug-in Manager

OfficeScan comporte une structure appelée Plug-in Manager qui intègre de nouvelles solutions dans l'environnement OfficeScan existant. Afin de faciliter la gestion de ces solutions, Plug-in Manager permet de voir en un coup d'œil les données correspondant aux solutions, sous forme de widgets.



Remarque

Actuellement, aucune des solutions de plug-in ne prend en charge IPv6. Le serveur peut télécharger ces solutions mais ne peut pas les déployer sur des agents OfficeScan IPv6 purs ni des hôtes IPv6 purs.

Plug-in Manager fournit deux types de solutions :

- **Fonctions natives du produit**

  Certaines fonctions natives d'OfficeScan possèdent une licence séparée et sont activées via Plug-in Manager. Dans cette version, deux fonctions entrent dans cette catégorie, respectivement **Trend Micro Virtual Desktop Support** et **Protection des données OfficeScan**.

- **Programmes plug-in**

  Les programmes de plug-in ne font pas partie du programme OfficeScan. Les modules additionnels disposent de licences et de consoles d'administration distinctes. Les consoles d'administration sont accessibles depuis la console Web OfficeScan. **Intrusion Defense Firewall**, **Trend Micro Security (for Mac)** et **Trend Micro Mobile Security** sont des exemples de modules additionnels.

Ce document fournit une présentation générale de l'installation et de la gestion des plug-ins et aborde les données relatives aux plug-ins disponibles dans les widgets. Reportez-vous à la documentation de chaque module additionnel pour plus d'informations sur la configuration et la gestion du programme.

Agents des modules additionnels sur des endpoints

Certains modules additionnels (tels qu'Intrusion Defense Firewall) disposent d'agents qui s'installent sur les systèmes d'exploitation Windows des endpoints. Le processus

Plug-in Manager des agents OfficeScan, qui s'exécute sous le nom de `CNTAoSMgr.exe`, gère ces endpoints.

OfficeScan installe `CNTAoSMgr.exe` en même temps que l'agent OfficeScan. Un seul programme supplémentaire est requis pour `CNTAoSMgr.exe` : Microsoft XML Parser (MSXML) version 3.0 ou ultérieure.



Remarque

D'autres modules additionnels disposent d'agents qui ne s'installent pas sous des systèmes d'exploitation Windows et ne sont pas gérés depuis le processus Plug-in Manager des agents OfficeScan. L'agent Trend Micro Security (for Mac) et l'agent dispositif Mobile pour Trend Micro Mobile Security sont de tels agents.

Widgets

Utilisez les widgets pour obtenir un aperçu global des données relatives aux solutions logicielles déployées. Les widgets sont disponibles sur le **Tableau de bord** du serveur OfficeScan. Un widget spécial, appelé **Mashup d'OfficeScan et des plug-ins**, combine les données des agents OfficeScan et des solutions modules additionnels, puis présente ces données dans l'arborescence des agents.

Le Manuel de l'administrateur fournit une présentation générale des widgets et des solutions qui prennent les widgets en charge.

Installation de Plug-in Manager

Dans les versions précédentes de Plug-in Manager, le package d'installation de Plug-in Manager était téléchargé à partir du serveur ActiveUpdate de Trend Micro, puis installé sur le endpoint hébergeant le serveur OfficeScan. Dans cette version, le pack d'installation de Plug-in Manager est compris dans le pack d'installation du serveur OfficeScan.

Lors de la toute première installation d'OfficeScan, le serveur OfficeScan et Plug-in Manager sont tous les deux installés. Lors de la mise à niveau d'OfficeScan vers cette

version et si les utilisateurs ont déjà utilisé Plug-in Manager, le service Plug-in Manager doit être arrêté avant l'exécution du package d'installation.

Exécution de tâches après l'installation

Après avoir installé Plug-in Manager, procédez comme suit :

Procédure

1. Ouvrez la console Web OfficeScan, puis cliquez sur **Modules additionnels** dans le menu principal.
2. Gérez les solutions de plug-in.
3. Accédez au **Tableau de bord** de la console Web OfficeScan pour gérer les widgets pour les solutions modules additionnels.

Gestion des fonctionnalités natives d'OfficeScan

Les fonctionnalités natives d'OfficeScan sont installées avec OfficeScan et peuvent être activées par les administrateurs à partir de Plug-in Manager. Certaines fonctionnalités, telles que Trend Micro Virtual Desktop Support, sont gérées depuis Plug-in Manager tandis que d'autres, telles que la protection des données OfficeScan, sont gérées depuis la console Web OfficeScan.

Gestion des modules additionnels

Installez et activez les modules additionnels indépendamment d'OfficeScan. Chaque module additionnel fournit sa propre console pour la gestion du produit. Les consoles de gestion sont accessibles depuis la console Web OfficeScan.

Installation de plug-ins

Les modules additionnels s'affichent dans la console **Plug-in Manager**. À partir de la console, vous pouvez télécharger, installer et gérer les programmes. Plug-In Manager télécharge le package d'installation d'un module additionnel à partir du serveur ActiveUpdate de Trend Micro ou d'une source de mise à jour personnalisée, si une source a été correctement configurée. Une connexion Internet est nécessaire pour télécharger le pack depuis le serveur ActiveUpdate.

Lorsque Plug-in Manager télécharge un package d'installation ou lance une installation, les fonctions des autres modules additionnels (téléchargements, installations et mises à niveau) sont temporairement désactivées.

Plug-in Manager ne prend pas en charge l'installation et la gestion d'un module additionnel via la fonction d'authentification unique de Trend Micro Control Manager.

Installation de modules additionnels

Procédure

1. Ouvrez la console Web OfficeScan, puis cliquez sur **Modules additionnels** dans le menu principal.

2. Sur l'écran **Plug-in Manager**, accédez à la section des modules additionnels et cliquez sur **Télécharger**.

   La taille du pack du module additionnel s'affiche en regard du bouton **Télécharger**. Plug-in Manager sauvegarde le package téléchargé dans le répertoire `<dossier d'installation du serveur>\PCCSRV\Download\Product`.

   Suivez la progression ou quittez cet écran pendant le téléchargement.

   Remarque

   Si OfficeScan rencontre des problèmes lors du téléchargement ou de l'installation du package, consultez les journaux de mise à jour du serveur sur la console Web OfficeScan. Dans le menu principal, cliquez sur **Journaux** > **Mise à jour du serveur**.

3. Cliquez sur **Installer maintenant** ou **Installer plus tard**.

- Une fois que vous avez cliqué sur **Installer maintenant**, l'installation commence et un écran de progression s'affiche.
- Une fois que vous avez cliqué sur **Installer plus tard**, l'écran **Plug-In Manager** s'affiche.

  Pour installer le module additionnel, cliquez sur le bouton **Installer** qui se trouve dans la section consacrée à ce module additionnel sur l'écran **Plug-in Manager**.

L'écran **Contrat de licence de l'utilisateur final Trend Micro** s'ouvre.



Remarque

Certains modules additionnels ne présentent pas un tel écran. Si cet écran ne s'affiche pas, l'installation du module additionnel commence.

4. Cliquez sur **J'accepte** pour installer le module additionnel.

   Suivez la progression ou quittez cet écran pendant l'installation.



Remarque

Si OfficeScan rencontre des problèmes lors du téléchargement ou de l'installation du package, consultez les journaux de mise à jour du serveur sur la console Web OfficeScan. Dans le menu principal, cliquez sur **Journaux** > **Mise à jour du serveur**.

Une fois l'installation terminée, la version actuelle du module additionnel s'affiche sur l'écran **Plug-In Manager**.

Activation de la licence d'un module additionnel

Procédure

1. Ouvrez la console Web OfficeScan, puis cliquez sur **Modules additionnels** dans le menu principal.
2. Sur l'écran **Plug-in Manager**, accédez à la section des modules additionnels et cliquez sur **Gestion de programme**.

L'écran **Nouveau code d'activation de la licence du produit** s'affiche.

3. Saisissez ou copiez-collez le code d'activation dans les champs de texte.

4. Cliquez sur **Enregistrer**.

   La console du module additionnel s'affiche.

Affichage et renouvellement des informations sur la licence

Procédure

1. Ouvrez la console Web OfficeScan, puis cliquez sur **Modules additionnels** dans le menu principal.

2. Sur l'écran **Plug-in Manager**, accédez à la section des modules additionnels et cliquez sur **Gestion de programme**.

3. Dans la console du module additionnel, accédez au lien hypertexte **Afficher les informations de licence**.

   Le lien hypertexte **Afficher les informations de licence** ne se trouve pas au même endroit pour tous les modules additionnels. Reportez-vous à la documentation de chaque module additionnel pour plus de détails.

4. Consultez les informations suivantes relatives à la licence dans l'écran qui s'ouvre.

OPTION	DESCRIPTION
État	Affiche « Activé », « Non activé » ou « Expiré ».
Version	Indique si la version est « Complète » ou d'« Évaluation ». **Remarque** Si la version finale et la version d'évaluation sont activées à la fois, seul « Complète » s'affiche.
Sièges	Affiche le nombre de endpoints pouvant être gérés par le module additionnel.

Option	Description
Date d'expiration du contrat de licence	Si un module additionnel dispose de plusieurs licences, la dernière date d'expiration s'affiche. Par exemple, si les dates d'expiration de la licence sont le 31/12/11 et le 30/06/11, la date qui s'affiche est le 31/12/11.
code d'activation	Affiche le code d'activation
Messages de rappel	Selon la version actuelle de votre licence, le module additionnel affiche des messages de rappel relatifs à la date d'expiration de la licence, soit durant la période de grâce (version complète uniquement), soit lorsque la licence expire.



Remarque

La durée de la période de grâce varie selon les régions. Consultez un représentant de Trend Micro pour connaître la période de grâce d'un module additionnel.

Lorsque la licence d'un module additionnel expire, ce dernier continue de fonctionner, mais plus aucune mise à jour n'a lieu et l'assistance n'est plus disponible.

5. Cliquez sur **Afficher le détail de la licence en ligne** pour afficher les informations relatives à la licence actuelle sur le site Web de Trend Micro.

6. Pour rafraîchir l'écran avec les dernières informations de licence, cliquez sur **Informations sur la mise à jour**.

7. Cliquez sur **Nouveau code d'activation** pour ouvrir l'écran **Nouveau code d'activation de la licence du produit**.

   Pour obtenir des informations détaillées, consultez la section *Activation de la licence d'un module additionnel à la page 3-4*.

Gestion des plug-ins

Configurez les paramètres et réalisez des tâches relatives à la console de gestion des plug-ins, accessible depuis la console Web OfficeScan. Ces tâches comprennent notamment l'activation du module additionnel et éventuellement le déploiement de son

agent sur les endpoints. Consultez la documentation spécifique du plug-in pour plus d'informations sur la configuration et la gestion du programme.

Gestion des modules additionnels

Procédure

1. Ouvrez la console Web OfficeScan, puis cliquez sur **Modules additionnels** dans le menu principal.

2. Sur l'écran **Plug-in Manager**, accédez à la section des modules additionnels et cliquez sur **Gestion de programme**.

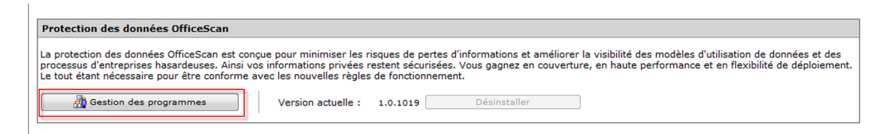


FIGURE 15-1. Bouton Gestion de programme

Lorsqu'un module additionnel est géré pour la première fois, il est possible que son activation soit nécessaire. Pour obtenir des informations détaillées, consultez la section *Activation de la licence d'un module additionnel à la page 3-4*.

Mises à niveau de plug-ins

La nouvelle version d'un module additionnel installé s'affiche dans la console de Plug-in Manager. Téléchargez le package, puis mettez à niveau le module additionnel sur la console. Plug-in Manager télécharge le package à partir du serveur ActiveUpdate de Trend Micro ou d'une source de mise à jour personnalisée (si une source a été correctement configurée). Une connexion Internet est nécessaire pour télécharger le pack depuis le serveur ActiveUpdate.

Lorsque Plug-in Manager télécharge un package d'installation ou lance une mise à niveau, il désactive temporairement les fonctions des autres modules additionnels (téléchargements, installations et mises à niveau).

Plug-in Manager ne prend pas en charge la mise à niveau de modules additionnels via la fonction d'authentification unique de Trend Micro Control Manager.

Mise à niveau des modules additionnels

Procédure

1. Ouvrez la console Web OfficeScan, puis cliquez sur **Modules additionnels** dans le menu principal.

2. Sur l'écran **Plug-in Manager**, accédez à la section des modules additionnels et cliquez sur **Télécharger**.

   La taille du pack de mise à niveau s'affiche en regard du bouton **Télécharger**.

   Suivez la progression ou quittez cet écran pendant le téléchargement.

   Remarque

   Si OfficeScan rencontre des problèmes lors du téléchargement ou de l'installation du package, consultez les journaux de mise à jour du serveur sur la console Web OfficeScan. Dans le menu principal, cliquez sur **Journaux** > **Mise à jour du serveur**.

3. Après que Plug-in Manager a terminé le téléchargement du pack, un nouvelle fenêtre s'affiche.

4. Cliquez sur **Mettre à niveau maintenant** ou **Mettre à niveau plus tard**.

   - Une fois que vous avez cliqué sur **Mettre à niveau maintenant**, la mise à niveau commence et un écran de progression s'affiche.

   - Une fois que vous avez cliqué sur **Mettre à niveau plus tard**, l'écran **Plug-In Manager** s'affiche.

     Pour mettre à niveau le module additionnel, cliquez sur le bouton **Mettre à niveau** qui se trouve dans la section consacrée à ce module additionnel sur l'écran **Plug-in Manager**.

Une fois la mise à niveau terminée, un redémarrage du service Plug-in Manager sera peut-être nécessaire. L'écran **Plug-in Manager** sera alors momentanément indisponible. Lorsque l'écran redevient disponible, la version actuelle du module additionnel s'affiche.

Désinstallation de plug-ins

Vous pouvez désinstaller un module additionnel de diverses manières :

- Désinstallez le module additionnel à partir de la console de Plug-in Manager.
- Désinstallez le serveur OfficeScan, ce qui désinstalle Plug-in Manager et tous les modules additionnels installés. Pour obtenir des instructions sur la désinstallation du serveur OfficeScan, consultez le *Guide d'installation et de mise à niveau OfficeScan*.

Pour les modules additionnels disposant d'agents sur le endpoint :

- Consultez la documentation relative au module additionnel pour savoir si sa désinstallation entraîne également la désinstallation de son agent.
- Quant aux agents des modules additionnels installés sur le même endpoint que l'agent OfficeScan, la désinstallation de l'agent OfficeScan entraîne la désinstallation des agents des modules additionnels et du processus Plug-in Manager (`CNTAoSMgr.exe`) de l'agent OfficeScan.

Désinstallation de modules additionnels à partir de la console de Plug-In Manager

Procédure

1. Ouvrez la console Web OfficeScan, puis cliquez sur **Modules additionnels** dans le menu principal.
2. Sur l'écran **Plug-in Manager**, accédez à la section des modules additionnels, puis cliquez sur **Désinstaller**.
3. Suivez la progression de la désinstallation ou quittez cet écran pendant la désinstallation.
4. Actualisez l'écran **Plug-in Manager** après la désinstallation.

Le plug-in est à nouveau prêt à être installé.

Uninstalling Plug-in Manager

Désinstallez le serveur OfficeScan afin de désinstaller Plug-in Manager et tous les plug-ins installés. Pour obtenir des instructions sur la désinstallation du serveur OfficeScan, consultez le *Guide d'installation et de mise à niveau OfficeScan*.

Dépannage de Plug-in Manager

Consultez les journaux de débogage du serveur OfficeScan et de l'agent OfficeScan pour obtenir des informations sur le débogage de Plug-In Manager et des modules additionnels.

Un module additionnel ne s'affiche pas dans la console de Plug-in Manager

Un module additionnel pouvant être téléchargé et installé peut ne pas s'afficher dans la console de Plug-in Manager pour les raisons suivantes :

Procédure

1. Plug-in Manager est toujours en train de télécharger le module additionnel. Le téléchargement peut prendre du temps selon la taille du pack du programme. Vérifiez l'écran de temps à autre pour voir si le module additionnel apparaît.



Remarque

Si Plug-in Manager n'est pas en mesure de télécharger le module additionnel, il procède à une nouvelle tentative au bout de 24 heures. Pour déclencher manuellement le téléchargement du module additionnel via Plug-in Manager, redémarrez le service OfficeScan Plug-in Manager.

2. Le serveur ne peut pas se connecter à Internet. Si le serveur se connecte à Internet par le biais d'un serveur proxy, assurez-vous que la connexion Internet peut être établie avec les paramètres proxy.

3. La source de mise à jour OfficeScan n'est pas le serveur ActiveUpdate. Dans la console Web OfficeScan, accédez à **Mises à jour** > **Serveur** > **Source de mise à jour** et vérifiez la source de mise à jour. Si la source de mise à jour ne correspond pas au serveur ActiveUpdate, plusieurs possibilités vous sont offertes :

    - Sélectionnez le serveur ActiveUpdate comme source de mise à jour.
    - Si vous sélectionnez **Autre source de mise à jour**, sélectionnez la première entrée comme source de mise à jour dans la liste **Autres sources de mise à jour**, puis vérifiez que la source peut correctement se connecter au serveur ActiveUpdate. Plug-in Manager ne prend en charge que la première entrée de la liste.
    - Si vous sélectionnez **Emplacement Intranet contenant une copie du fichier actuel**, assurez-vous que le endpoint qui se trouve sur l'intranet peut également se connecter au serveur ActiveUpdate.

Problèmes d'installation et d'affichage de l'agent des modules additionnels sur des endpoints

L'installation de l'agent des modules additionnels sur le endpoint peut échouer ou l'agent peut ne pas s'afficher dans la console de l'agent OfficeScan pour les raisons suivantes :

Procédure

1. Plug-in Manager (`CNTAosMgr.exe`) ne s'exécute pas sur le endpoint. Sur le endpoint de l'agent OfficeScan, ouvrez le Gestionnaire de tâches de Windows et exécutez le processus `CNTAosMgr.exe`.

2. Le package d'installation de l'agent des modules additionnels n'a pas été téléchargé dans le dossier du endpoint de l'agent OfficeScan situé dans le répertoire `<dossier d'installation de l'agent>\AU_Data\AU_Temp\{xxx}AU_Down\Product`. Consultez `Tmudump.txt` situé dans `\AU_Data\AU_Log\` pour connaître les raisons de l'échec du téléchargement.



Remarque

Si un agent est installé avec succès, des informations sur cet agent sont disponibles dans le fichier `<dossier d'installation de l'agent>\AOSSvcInfo.xml`.

3. L'installation de l'agent a échoué ou nécessite d'autres actions. Vous pouvez vérifier l'état de l'installation à partir de la console d'administration du module additionnel et procéder à un redémarrage du endpoint de l'agent OfficeScan à la fin de l'installation, ou encore installer des mises à jour système avant de procéder à l'installation.

Cette version du serveur Web Apache n'est pas prise en charge

Plug-in Manager traite certaines requêtes Internet à l'aide de l'interface ISAPI (Internet Server Application Programming Interface). L'interface ISAPI n'est pas compatible avec le serveur Web Apache versions 2.0.56 à 2.0.59 et versions 2.2.3 à 2.2.4.

Si vous avez une version incompatible du serveur Web Apache, vous pouvez le remplacer par la version 2.2.25, qui est utilisée par OfficeScan et Plug-in Manager. Cette version est également compatible avec l'interface ISAPI.

Procédure

1. Mettez à niveau le serveur OfficeScan vers la version actuelle.
2. Sauvegardez les fichiers suivants dans le dossier Apache2 du `<dossier d'installation du serveur>` :
   - `httpd.conf`
   - `httpd.conf.tmbackup`
   - `httpd.default.conf`
3. Désinstallez la version incompatible du serveur Web Apache depuis l'écran **Ajout/ Suppression de programmes**.
4. Installer le serveur Web Apache 2.2.25

a. Lancez `apache.msi` à partir du répertoire `<dossier d'installation du serveur>\Admin\Utility\Apache`.

b. Dans l'écran relatif aux informations du serveur, entrez les informations demandées.

c. Dans l'écran Dossier de destination, modifiez le dossier de destination en cliquant sur **Modifier** et en accédant au `<dossier d'installation du serveur>`.

d. Terminez l'installation.

5. Copiez les fichiers de sauvegarde dans le dossier Apache2.

6. Redémarrez le service serveur Web Apache.

Lancement impossible des agents sur des endpoints si le paramètre du script de configuration automatique dans Internet Explorer redirige vers un serveur proxy

Le processus Plug-in Manager (`CNTAosMgr.exe`) des agents OfficeScan ne peut pas lancer d'agents sur les endpoints car la commande de lancement de l'agent entraîne une redirection vers un serveur proxy. Le problème ne survient que si les paramètres proxy redirigent le trafic HTTP de l'utilisateur vers le port 127.0.0.1.

Pour résoudre ce problème, utilisez une stratégie de serveur proxy bien définie. Par exemple, ne redirigez pas le trafic HTTP vers le port 127.0.0.1.

Si vous devez utiliser la configuration proxy contrôlant les requêtes HTTP 127.0.0.1, effectuez les tâches suivantes :

Procédure

1. Configurez les paramètres du pare-feu OfficeScan dans la console Web OfficeScan.



Remarque

Réalisez cette opération uniquement si vous activez le pare-feu OfficeScan sur les agents OfficeScan.

a. Dans la console Web, accédez à **Agents** > **Pare-feu** > **Stratégies** et cliquez sur **Modifier le modèle d'exception**.

b. Dans l'écran Modifier le modèle d'exception, cliquez sur **Ajouter**.

c. Utilisez les informations suivantes :

- **Nom** : le nom de votre choix
- **Action** : Autoriser le trafic réseau
- **Direction** : Entrant
- **Protocole** : TCP
- **Port(s)** : Tout numéro de port compris entre 5000 et 49151

d. **Adresse(s) IP** : Sélectionnez **Adresse IP unique** et spécifiez l'adresse IP de votre serveur proxy (recommandé) ou sélectionnez **Toutes les adresses IP**.

e. Cliquez sur **Enregistrer**.

f. De retour dans l'écran Modifier le modèle d'exception, cliquez sur **Enregistrer et appliquer aux stratégies existantes**.

g. Accédez à **Agents** > **Pare-feu** > **Profils**, puis cliquez sur **Affecter un profil aux agents**.

S'il n'existe pas de profil de pare-feu, créez-en un en cliquant sur Ajouter. Utilisez les paramètres suivants :

- **Nom** : le nom de votre choix
- **Description**: la description de votre choix
- **Stratégie** : Toutes les stratégies d'accès

Une fois le nouveau profil enregistré, cliquez sur **Affecter un profil aux agents**.

2. Modifiez le fichier `ofcscan.ini`.

a. Ouvrez le fichier `ofcscan.ini` situé dans le `<Dossier d'installation du serveur>` via un éditeur de texte.

b. Recherchez **[Global Setting]** et ajoutez `FWPortNum=21212` à la ligne suivante. Remplacez la valeur « 21212 » par le numéro de port précédemment spécifié à l'étape c.

Par exemple :

```
[Global Setting]
```

```
FWPortNum=5000
```

c. Enregistrez le fichier.

3. Sur la console Web, accédez à **Agents** > **Paramètres généraux de l'agent** et cliquez sur **Enregistrer**.

Une erreur s'est produite dans le système, le module de mise à jour ou le programme Plug-in Manager et le message d'erreur fournit un certain code d'erreur

Plug-in Manager affiche l'un des codes d'erreur suivants dans un message d'erreur. Si vous ne parvenez pas à résoudre un problème après avoir consulté les solutions proposées dans le tableau ci-dessous, adressez-vous à votre service d'assistance.

Tableau 15-1. Codes d'erreur de Plug-In Manager

Code d'erreur	Message, cause et solution
001	Une erreur est survenue dans le programme Plug-in Manager. Le module de mise à jour de Plug-in Manager ne répond pas lors de l'interrogation de la progression d'une tâche de mise à jour. Le gestionnaire de commande ou de module n'a peut-être pas été initialisé. Redémarrez le service Plug-in Manager d'OfficeScan, puis exécutez à nouveau la tâche.

Code d'erreur	Message, cause et solution
002	Une erreur système est survenue. Le module de mise à jour de Plug-In Manager ne parvient pas à ouvrir la clé de Registre `SOFTWARE\TrendMicro\OfficeScan\service\AoS` car elle a été supprimée. Effectuez les actions suivantes : 1. Ouvrez l'Éditeur du Registre et accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_Addon_Service_CompList_Version`. Redéfinissez la valeur sur 1.0.1000. 2. Redémarrez le service OfficeScan Plug-in Manager. 3. Téléchargez/désinstallez le plug-in.

<table>
<tr><th>CODE D'ERREUR</th><th>MESSAGE, CAUSE ET SOLUTION</th></tr>
<tr><td>028</td><td>Une erreur de mise à jour est survenue.

Causes possibles :

• Le module de mise à jour de Plug-in Manager n'a pas pu télécharger de module additionnel. Vérifiez que la connexion réseau fonctionne correctement, puis réessayez.

• Le module de mise à jour de Plug-in Manager ne peut pas installer le module additionnel car l'agent de patch AU a renvoyé une erreur. L'agent du patch AU est le programme qui lance l'installation des nouveaux modules additionnels. Pour connaître la cause exacte de l'erreur, consultez le journal de débogage du module « TmuDump.txt » dans \PCCSRV\Web\Service\AU_Data\AU_Log.

Effectuez les actions suivantes :

1. Ouvrez l'Éditeur du Registre et accédez à HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_Addon_Service_CompList_Version. Redéfinissez la valeur sur 1.0.1000.

2. Supprimez la clé de registre du module additionnel HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_ADDON_xxxx.

3. Redémarrez le service OfficeScan Plug-in Manager.

4. Téléchargez et installez le module additionnel.</td></tr>
<tr><td>170</td><td>Une erreur système est survenue.

Le module de mise à jour de Plug-in Manager ne peut pas traiter d'opération entrante car il est actuellement en train de traiter une autre opération.

Veuillez effectuer cette tâche ultérieurement.</td></tr>
<tr><td>202</td><td>Une erreur est survenue dans le programme Plug-in Manager.

Plug-in Manager ne peut pas traiter une tâche en cours d'exécution sur la console Web.

Actualisez la console Web ou mettez à niveau Plug-in Manager si une mise à niveau est disponible.</td></tr>
</table>

Code d'erreur	Message, cause et solution
203	Une erreur est survenue dans le programme Plug-in Manager. Le programme Plug-in Manager a rencontré une erreur de communication inter-processus (IPC) lors d'une tentative de communication avec les services back-end de Plug-in Manager. Redémarrez le service Plug-in Manager d'OfficeScan, puis exécutez à nouveau la tâche.
Autres codes d'erreur	Une erreur système est survenue. Lors du téléchargement d'un nouveau module additionnel, Plug-in Manager vérifie la liste des modules additionnels à partir du serveur ActiveUpdate. Plug-in Manager n'a pas été en mesure d'obtenir la liste. Effectuez les actions suivantes : 1. Ouvrez l'Éditeur du Registre et accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_Addon_Service_CompList_Version`. Redéfinissez la valeur sur `1.0.1000`. 2. Redémarrez le service OfficeScan Plug-in Manager. 3. Téléchargez et installez le module additionnel.



Chapitre 16

Ressources de dépannage

Ce chapitre met à votre disposition une liste de ressources qui permettent de résoudre les problèmes liés au serveur OfficeScan et aux agents OfficeScan.

Les rubriques sont les suivantes :

Assistance Intelligence System

Support Intelligence System est une page depuis laquelle vous pouvez facilement envoyer des fichiers à Trend Micro à des fins d'analyse. Ce système détecte le GUID du serveur OfficeScan et joint cette information au fichier que vous envoyez. En joignant ce GUID, vous permettez à Trend Micro de vous fournir un retour d'informations sur les fichiers envoyés pour évaluation.

Case Diagnostic Tool

Trend Micro Case Diagnostic Tool (CDT) collecte les informations de débogage nécessaires issues du produit d'un client à chaque fois qu'un problème apparaît. Il active ou désactive automatiquement le débogage du produit et collecte les fichiers nécessaires en fonction des catégories de problèmes. Trend Micro utilise ces informations pour résoudre les problèmes liés au produit.

Exécutez l'outil sur toutes les plates-formes prises en charge par OfficeScan. Pour obtenir cet outil et la documentation appropriée, contactez votre service d'assistance.

Trend Micro Performance Tuning Tool

Trend Micro fournit un outil autonome d'optimisation des performances pour identifier les applications susceptibles de provoquer des problèmes de performances. Trend Micro Performance Tuning Tool, disponible dans la base de connaissances de Trend Micro, doit être exécuté sur une image de poste de travail autonome et/ou sur quelques postes de travail cibles durant le processus pilote pour éviter les problèmes de performances dans le déploiement réel de la surveillance des comportements et du contrôle des dispositifs.

Pour plus d'informations, visitez le site http://esupport.trendmicro.com/solution/en-us/1056425.aspx.

Journaux du serveur OfficeScan

En plus des journaux disponibles sur la console Web, vous pouvez utiliser d'autres types de journaux (tels que les journaux de débogage) pour résoudre les problèmes liés aux produits.



AVERTISSEMENT!

Les journaux de débogage risquent de diminuer les performances du serveur et utilisent une quantité considérable d'espace disque. Activez la journalisation du débogage si nécessaire et désactivez-la immédiatement si vous n'utilisez plus les données de débogage. Supprimez le fichier journal si vous avez besoin d'espace disque.

Journaux de débogage du serveur à l'aide de LogServer.exe

Utilisez `LogServer.exe` afin de collecter les journaux de débogage pour les entités suivantes :

- Journaux de base du serveur OfficeScan
- Trend Micro Vulnerability Scanner
- Journaux d'intégration d'Active Directory
- Journaux de regroupement des agents
- Journaux de conformité de la sécurité
- Administration basée sur les rôles
- Smart scan

Activation de la journalisation du débogage

Procédure

1. Connectez-vous à la console Web.

2. Dans la bannière de la console Web, cliquez sur le premier « O » dans « OfficeScan ».

3. Spécifiez les paramètres de journalisation du débogage.

4. Cliquez sur **Enregistrer**.

5. Vérifiez le fichier journal (`ofcdebug.log`) dans son emplacement par défaut : <*dossier d'installation du serveur*>`\PCCSRV\Log`.

Désactivation de la journalisation du débogage

Procédure

1. Connectez-vous à la console Web.

2. Dans la bannière de la console Web, cliquez sur le premier « O » dans « OfficeScan ».

3. Désactivez **Activer le journal de débogage**.

4. Cliquez sur **Enregistrer**.

Activation de la journalisation du débogage pour l'installation et la mise à niveau du serveur

Activez la journalisation du débogage avant d'exécuter les tâches suivantes:

- Désinstaller et réinstaller le serveur.
- Procéder à une mise à niveau d'OfficeScan vers une nouvelle version.
- Exécuter une installation/mise à niveau à distance (la journalisation du débogage est activée sur le endpoint sur lequel vous avez lancé le programme d'installation et non sur le endpoint distant).

Procédure

1. Copiez le dossier `LogServer` situé dans le répertoire <*dossier d'installation du serveur*>`\PCCSRV\Private` dans `C:\`.
2. Créez un fichier nommé `cdebug.ini` avec le contenu suivant :

```
[debug]

debuglevel=9

debuglog=c:\LogServer\ofcdebug.log

debugLevel_new=D

debugSplitSize=10485760

debugSplitPeriod=12

debugRemoveAfterSplit=1
```

3. Enregistrez `ofcdebug.ini` dans `C:\LogServer`.
4. Exécutez la tâche appropriée (c'est-à-dire, désinstaller/réinstaller le serveur, mettre à niveau vers une nouvelle version ou exécuter une installation/mise à niveau à distance).
5. Vérifiez le fichier `ofcdebug.log` dans `C:\LogServer`.

Journaux d'installation

- Journaux d'installation/de mise à niveau locale

  Nom du fichier : `OFCMAS.LOG`

  Emplacement : `%windir%`

- Journaux d'installation/de mise à niveau à distance

  - Sur le endpoint sur lequel vous avez lancé le programme d'installation :

    Nom du fichier : `ofcmasr.log`

Emplacement : `%windir%`

- Sur le endpoint cible :

  Nom du fichier : `OFCMAS.LOG`

  Emplacement : `%windir%`

Journaux Active Directory

- Nom du fichier : `ofcdebug.log`
- Nom du fichier : `ofcserver.ini`

  Emplacement : <*dossier d'installation du serveur*>`\PCCSRV\Private\`
- Noms de fichiers :
  - `dbADScope.cdx`
  - `dbADScope.dbf`
  - `dbADPredefinedScope.cdx`
  - `dbADPredefinedScope.dbf`
  - `dbCredential.cdx`
  - `dbCredential.dbf`

  Emplacement : `<dossier d'installation du serveur>\PCCSRV\HTTPDB\`

Journaux de Role-based Administration

Pour des informations détaillées sur l'administration basée sur les rôles, effectuez l'une des opérations suivantes:

- Lancez Trend Micro Case Diagnostics Tool. Pour plus d'informations, consultez *Case Diagnostic Tool à la page 16-2*.
- Rassemblez les journaux suivants:

- Tous les fichiers qui se trouvent dans le répertoire <*dossier d'installation du serveur*>\PCCSRV\Private\AuthorStore.
- *Journaux du serveur OfficeScan à la page 16-3*

Journaux de regroupement des agents OfficeScan

- Nom du fichier : ofcdebug.log
- Nom du fichier : ofcserver.ini

  Emplacement : <*dossier d'installation du serveur*>\PCCSRV\Private\
- Nom du fichier : SortingRule.xml

  Emplacement : <dossier d'installation du serveur>\PCCSRV\Private\SortingRuleStore\
- Noms de fichiers :
  - dbADScope.cdx
  - dbADScope.dbf

  Emplacement : <dossier d'installation du serveur>\HTTPDB\

Journaux de mise à jour des composants

Nom du fichier : TmuDump.txt

Emplacement : <*dossier d'installation du serveur*>\PCCSRV\Web\Service\AU_Data\AU_Log

Obtention d'informations détaillées sur la mise à jour du serveur

Procédure

1. Créez un fichier nommé aucfg.ini avec le contenu suivant :

```
[Debug]

level=-1

[Downloader]

ProxyCache=0
```

2. Enregistrez le fichier dans le répertoire <*dossier d'installation du serveur*>`\PCCSRV\Web\Service`.

3. Redémarrez le service principal d'OfficeScan.

Arrêt de la collecte d'informations détaillées sur la mise à jour du serveur

---

Procédure

1. Supprimez le fichier `aucfg.ini`.

2. Redémarrez le service principal d'OfficeScan.

Journaux du serveur Apache

Noms de fichiers :

- `install.log`
- `error.log`
- `access.log`

Emplacement : <*dossier d'installation du serveur*>`\PCCSRV\Apache2`

Journaux d'Agent Packager

Activation de la journalisation pour la création d'Agent Packager

Procédure

1. Modifiez le fichier `ClnExtor.ini` qui se trouve dans le répertoire <*dossier d'installation du serveur*>`\PCCSRV\Admin\Utility\ClientPackager`comme suit :

   `[Common]`

   `DebugMode=1`

2. Vérifiez le fichier `ClnPack.log` dans `C:\`.

Désactivation de la journalisation pour la création d'Agent Packager

Procédure

1. Ouvrez le fichier `ClnExtor.ini`.
2. Remplacez la valeur 1 de « DebugMode » par 0.

Journaux de rapport de conformité de la sécurité

Pour obtenir des informations détaillées sur la conformité de la sécurité, rassemblez les informations suivantes :

- Nom du fichier : `RBAUserProfile.ini`

  Emplacement : <*dossier d'installation du serveur*>`\PCCSRV\Private\AuthorStore\`

- Tous les fichiers du répertoire `<dossier d'installation du serveur>\PCCSRV\Log\Security Compliance Report`.
- *Journaux du serveur OfficeScan à la page 16-3*

Journaux de gestion des serveurs externes

- Nom du fichier : `ofcdebug.log`
- Nom du fichier : `ofcserver.ini`

  Emplacement : <*dossier d'installation du serveur*>`\PCCSRV\Private\`
- Tous les fichiers du répertoire `<dossier d'installation du serveur>\PCCSRV\Log\Outside Server Management Report\`.
- Noms de fichiers:
  - `dbADScope.cdx`
  - `dbADScope.dbf`
  - `dbClientInfo.cdx`
  - `dbclientInfo.dbf`

  Emplacement : `<dossier d'installation du serveur>\HTTPDB\`

Journaux d'exceptions du contrôle des dispositifs

Pour obtenir des informations détaillées sur les exceptions du contrôle des dispositifs, rassemblez les informations suivantes :

- Nom du fichier : `ofcscan.ini`

  Emplacement : <*dossier d'installation du serveur*>`\`
- Nom du fichier : `dbClientExtra.dbf`

  Emplacement : `<dossier d'installation du serveur>\HTTPDB\`

- Liste d'exceptions du contrôle des dispositifs sur la console Web d'OfficeScan.

Journaux de réputation de sites Web

Nom du fichier : `diagnostic.log`

Emplacement : <*dossier d'installation du serveur*>`\PCCSRV\LWCS\`

Journaux de l'outil ServerProtect Normal Server Migration

Pour activer la journalisation du débogage pour l'outil ServerProtect Normal Server Migration:

Procédure

1. Créez un fichier nommé `ofcdebug.ini` avec le contenu suivant :

```
[Debug]

DebugLog=C:\ofcdebug.log

DebugLevel=9
```

2. Enregistrez le fichier sous `C:\`.

3. Vérifiez le fichier `ofcdebug.log` dans `C:\`.



Remarque

Pour désactiver la journalisation du débogage, supprimez le fichier `ofcdebug.ini`.

Journaux de VSEncrypt

OfficeScan crée automatiquement ce journal de débogage (`VSEncrypt.log`) dans le dossier temporaire du compte utilisateur. Par exemple, dans `C:\Documents and Settings\<Nom de l'utilisateur>\Local Settings\Temp`.

Journaux de l'agent MCP de Control Manager

Fichiers de débogage situés dans le répertoire <*dossier d'installation du serveur*>`\PCCSRV\CMAgent`

- `Agent.ini`
- `Product.ini`
- Capture d'écran de la page des paramètres de Control Manager
- `ProductUI.zip`

Activation de la journalisation du débogage pour l'agent MCP

Procédure

1. Modifiez le fichier `product.ini` qui se trouve dans le répertoire <*dossier d'installation du serveur*>`\PCCSRV\CmAgent` comme suit :

```
[Debug]

debugmode = 3

debuglevel= 3

debugtype = 0

debugsize = 10000

debuglog = C:\CMAgent_debug.log
```

2. Redémarrez le service Control Manager Agent d'OfficeScan depuis Microsoft Management Console.

3. Vérifiez le fichier `CMAgent_debug.log` dans `C:\`.

Désactivation de la journalisation du débogage pour l'agent MCP

Procédure

1. Ouvrez le fichier `product.ini` et supprimez les éléments suivants :

   ```
   debugmode = 3

   debuglevel= 3

   debugtype = 0

   debugsize = 10000

   debuglog = C:\CMAgent_debug.log
   ```

2. Redémarrez le service OfficeScan Control Manager.

Journaux du moteur de scan antivirus

Pour activer la journalisation du débogage pour le moteur de scan antivirus:

Procédure

1. Ouvrez l'éditeur de la base de registre (`regedit.exe`).
2. Accédez à `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMFilter\Parameters`.
3. Remplacez la valeur de la variable « `DebugLogFlags` » par « `00003eff` ».
4. Exécutez les étapes ayant mené au problème de scan que vous avez rencontré.
5. Vérifiez le fichier `TMFilter.log` dans `%windir%`.



Remarque

Désactivez la journalisation du débogage en réaffectant à la variable « `DebugLogFlags` » la valeur « `00000000` »

Journaux de virus/programmes malveillants

Nom du fichier :

- `dbVirusLog.dbf`
- `dbVirusLog.cdx`

Emplacement : <*dossier d'installation du serveur*>`\PCCSRV\HTTPDB\`

Journaux de spywares/graywares

Nom du fichier :

- `dbSpywareLog.dbf`
- `dbSpywareLog.cdx`

Emplacement : <*dossier d'installation du serveur*>`\PCCSRV\HTTPDB\`

Journaux des épidémies

Type de journal	Fichier
Journaux actuels des épidémies de violation de pare-feu	Nom du fichier : `Cfw_Outbreak_Current.log` Emplacement : <*dossier d'installation du serveur*>`\PCCSRV\Log`
Derniers journaux des épidémies de violation de pare-feu	Nom du fichier : `Cfw_Outbreak_Last.log` Emplacement : <*dossier d'installation du serveur*>`\PCCSRV\Log`

TYPE DE JOURNAL	FICHIER
Journaux actuels des épidémies de virus/ programmes malveillants	Nom du fichier : Outbreak_Current.log Emplacement : <*dossier d'installation du serveur*>\PCCSRV \Log
Derniers journaux des épidémies de virus/ programmes malveillants	Nom du fichier : Outbreak_Last.log Emplacement : <*dossier d'installation du serveur*>\PCCSRV \Log
Journaux actuels des épidémies de spywares/ graywares	Nom du fichier : Spyware_Outbreak_Current.log Emplacement : <*dossier d'installation du serveur*>\PCCSRV \Log
Derniers journaux des épidémies de spywares/ graywares	Nom du fichier : Spyware_Outbreak_Last.log Emplacement : <*dossier d'installation du serveur*>\PCCSRV \Log

Journaux de Virtual Desktop Support

- Nom du fichier : `vdi_list.ini`

  Emplacement : <*dossier d'installation du serveur*>\PCCSRV\TEMP

- Nom du fichier : `vdi.ini`

  Emplacement : <dossier d'installation du serveur>\PCCSRV \Private\

- Nom du fichier : `ofcdebug.txt`

  Emplacement : <dossier d'installation du serveur>\PCCSRV\

Pour générer `ofcdebug.txt`, activez la journalisation du débogage. Pour plus d'informations sur l'activation de la journalisation du débogage, voir *Activation de la journalisation du débogage à la page 16-3*.

Journaux des agents OfficeScan

Utilisez les journaux des agents OfficeScan (tels que les journaux de débogage) pour résoudre les problèmes liés aux agents OfficeScan.



AVERTISSEMENT!

Les journaux de débogage risquent de diminuer les performances des agents et utilisent une quantité considérable d'espace disque. Activez la journalisation du débogage si nécessaire et désactivez-la immédiatement si vous n'utilisez plus les données de débogage. Supprimez le fichier journal si la taille du fichier devient trop volumineuse.

Journaux de débogage des agents OfficeScan à l'aide de LogServer.exe

Pour activer la journalisation du débogage pour l'agent OfficeScan :

Procédure

1. Créez un fichier nommé `ofcdebug.ini` avec le contenu suivant :

```
[Debug]

Debuglog=C:\ofcdebug.log

debuglevel=9

debugLevel_new=D

debugSplitSize=10485760

debugSplitPeriod=12

debugRemoveAfterSplit=1
```

2. Envoyez le fichier `ofcdebug.ini` aux utilisateurs, en leur demandant de l'enregistrer sous `C:\`.



Remarque

`LogServer.exe` s'exécute automatiquement à chaque redémarrage du endpoint de l'agent OfficeScan. Demandez aux utilisateurs de ne PAS fermer la fenêtre de commande de LogServer.exe qui s'ouvre au démarrage du endpoint, car cette opération invite OfficeScan à interrompre la journalisation du débogage. Si les utilisateurs ferment la fenêtre de commande, ils peuvent relancer la journalisation du débogage en exécutant `LogServer.exe` depuis le <*dossier d'installation de l'agent*>.

3. Pour chaque endpoint de l'agent OfficeScan, vérifiez le fichier ofcdebug.log dans C:\.



Remarque

Désactivez la journalisation du débogage pour l'agent OfficeScan en supprimant le fichier `ofcdebug.ini`.

Journaux des nouvelles installations

Nom du fichier : `OFCNT.LOG`

Emplacements :

- `%windir%` pour toutes les méthodes d'installation à l'exception du pack MSI
- `%temp%` pour la méthode d'installation à l'aide du pack MSI

Journaux des mises à niveau/correctifs de type hotfix

Nom du fichier : `upgrade_yyyymmddhhmmss.log`

Emplacement : <*dossier d'installation de l'agent*>`\Temp`

Journaux de Damage Cleanup Services

Activation de la journalisation du débogage pour Damage Cleanup Services

Procédure

1. Ouvrez le fichier `TSC.ini` qui se trouve dans le <*dossier d'installation de l'agent*>.

2. Modifiez la ligne suivante comme suit:

   `DebugInfoLevel=3`

3. Vérifiez le fichier `TSCDebug.log` qui se trouve dans le répertoire `<dossier d'installation de l'agent>\debug`.

Activation de la journalisation du débogage pour Damage Cleanup Services

Ouvrez le fichier `TSC.ini` et remplacez la valeur 3 de la variable « `DebugInfoLevel` » par 0.

Journal Cleanup

Nom du fichier : `yyyymmdd.log`

Emplacement : <*dossier d'installation de l'agent*>`\report\`

Journaux de scan de courrier

Nom du fichier : `SmolDbg.txt`

Emplacement : <*dossier d'installation de l'agent*>

Journaux de connexion des agents OfficeScan

Nom du fichier : `Conn_YYYYMMDD.log`

Emplacement : <*dossier d'installation de l'agent*>`\ConnLog`

Journaux de mise à jour des agents OfficeScan

Nom du fichier : `Tmudump.txt`

Emplacement : <*dossier d'installation de l'agent*>`\AU_Data\AU_Log`

Obtention d'informations détaillées sur les mises à jour des agents OfficeScan

Procédure

1. Créez un fichier nommé `aucfg.ini` avec le contenu suivant :

```
[Debug]

level=-1

[Downloader]

ProxyCache=0
```

2. Enregistrez le fichier dans le <*dossier d'installation de l'agent*>.

3. Rechargez l'agent OfficeScan.



Remarque

Cessez de collecter les informations détaillées sur les mises à jour de l'agent en supprimant le fichier `aucfg.ini` et en rechargeant l'agent OfficeScan.

Journaux de prévention des épidémies

Nom du fichier : `OPPLogs.log`

Emplacement : <*dossier d'installation de l'agent*>`\OppLog`

Journaux de rétablissement de la prévention des épidémies

Noms de fichiers :

- `TmOPP.ini`
- `TmOPPRestore.ini`

Emplacement : <*dossier d'installation de l'agent*>`\`

Journaux du pare-feu OfficeScan

Activation de la journalisation du débogage pour le pilote du pare-feu commun sur les ordinateurs Windows Vista/Server 2008/7/Server 2012/8/8.1

Procédure

1. Modifiez les valeurs de registre suivantes :

CLÉ DE REGISTRE	VALEURS
`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmwfp\Parameters`	Type : Valeur `DWORD (REG_DWORD)` Nom : `DebugCtrl` Valeur : `0x00001111`

Clé de registre	Valeurs
HKEY_LOCAL_MACHINE\System\CurrentControlSet \Services\tmlwf\Parameters	Type : Valeur DWORD (REG_DWORD) Nom : DebugCtrl Valeur : 0x00001111

2. Redémarrez le endpoint.

3. Vérifiez les fichiers wfp_log.txt et lwf_log.txt dans C:\.

Activation de la journalisation du débogage pour le pilote de pare-feu commun sur les ordinateurs Windows XP et Windows Server 2003

Procédure

1. Ajoutez les données suivantes dans HKEY_LOCAL_MACHINE\System \CurrentControlSet\Services\tmcfw\Parameters :

   - Type : Valeur DWORD (REG_DWORD)
   - Nom : DebugCtrl
   - Valeur : 0x00001111

2. Redémarrez le endpoint.

3. Vérifiez le fichier cfw_log.txt dans C:\.

Désactivation de la journalisation du débogage pour Pilote du pare-feu commun (tous les systèmes d'exploitation)

Procédure

1. Supprimez « DebugCtrl » dans la clé de registre.

2. Redémarrez le endpoint.

Activation de la journalisation du débogage pour le service de pare-feu OfficeScan NT

Procédure

1. Modifiez le fichier `TmPfw.ini` qui se trouve dans le <*dossier d'installation de l'agent*> comme suit :

   `[ServiceSession]`

   `Enable=1`

2. Rechargez l'agent.

3. Vérifiez `ddmmyyyy_NSC_TmPfw.log` dans `C:\temp`.

Désactivation de la journalisation du débogage pour le service de pare-feu OfficeScan NT

Procédure

1. Ouvrez le fichier `TmPfw.ini` et remplacez la valeur 1 de la variable « `Enable` » par 0.

2. Rechargez l'agent OfficeScan.

Journaux de la réputation de sites Web et du scan de la messagerie POP3

Activation de la journalisation du débogage pour les fonctions de réputation de sites Web et de scan de la messagerie POP3

Procédure

1. Modifiez le fichier `TmProxy.ini` qui se trouve dans le <*dossier d'installation de l'agent*> comme suit :

   ```
   [ServiceSession]

   Enable=1

   LogFolder=C:\temp
   ```

2. Rechargez l'agent OfficeScan.

3. Vérifiez `ddmmyyyy_NSC_TmProxy.log` dans `C:\temp`.

Désactivation de la journalisation du débogage pour les fonctions de réputation de sites Web et de scan de la messagerie POP3

Procédure

1. Ouvrez le fichier `TmProxy.ini` et remplacez la valeur 1 de la variable « `Enable` » par 0.

2. Rechargez l'agent OfficeScan.

Journaux de listes d'exceptions du contrôle des dispositifs

Nom du fichier : DAC_ELIST

Emplacement : <*dossier d'installation de l'agent*>\

Journaux de débogage de protection des données

Pour activer les journaux de débogage de la protection des données :

Procédure

1. Obtenez le fichier logger.cfg auprès de votre service d'assistance.
2. Ajoutez les données suivantes dans HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\DlpLite:
   - Type : chaîne
   - Nom : debugcfg
   - Valeur : C:\Log\logger.cfg
3. Créez un dossier intitulé « Log » dans le C:\ directory.
4. Copiez le fichier logger.cfg dans le dossier Log.
5. Déployez la prévention contre la perte des données et les paramètres de contrôle des dispositifs depuis la console Web pour lancer la collecte de journaux.



Remarque

Désactivez la journalisation de débogage pour le module Protection des données en supprimant debugcfg dans la clé de Registre et en redémarrant le endpoint.

Journaux des événements Windows

L'Observateur d'événements de Windows affiche les événements d'application, tels que les connexions ou les modifications de paramètres de compte.

Procédure

1. Effectuez l'une des actions suivantes:
   - Cliquez sur **Démarrer** > **Panneau de configuration** > **Performances et maintenance** > **Outils administrateurs** > **Gestion de l'ordinateur**.
   - Ouvrez MMC, qui contient le composant logiciel enfichable Observateur d'événements.
2. Cliquez sur **Observateur d'événements**.

Journaux de l'interface Transport Driver Interface (TDI)

Pour activer les journaux de l'interface Transport Driver Interface (TDI) :

Procédure

1. Ajoutez les données suivantes dans `HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Service\tmtdi\Parameters` :

PARAMÈTRE	VALEURS
Clé 1	Type : Valeur `DWORD (REG_DWORD)` Nom : `Déboguer` Valeur : `1111 (hexadécimal)`
Clé 2	Type : `valeur de chaîne (REG_SZ)` Nom : `LogFile` Valeur : `C:\tmtdi.log`

2. Redémarrez le endpoint.

3. Vérifiez le fichier `tmtdi.log` dans `C:\`.



Remarque

Désactivez la journalisation du débogage pour TDI en supprimant `Debug` et `LogFile` dans la clé de Registre, puis redémarrez le endpoint.



Chapitre 17

Assistance technique

Ce chapitre explique comment trouver des solutions en ligne, utiliser le portail d'assistance et contacter Trend Micro.

Les rubriques sont les suivantes :

Ressources de dépannage

Avant de contacter le service d'assistance technique, consultez les ressources d'aide en ligne suivantes fournies par Trend Micro.

Trend Community

Pour obtenir de l'aide, partager des expériences, poser des questions et discuter de vos inquiétudes quant aux problèmes de sécurité avec d'autres utilisateurs, des amateurs et des experts, rendez-vous sur le site :

http://community.trendmicro.com/

Utilisation du portail d'assistance

Le portail d'assistance de Trend Micro est une ressource en ligne disponible 24 h/24 et 7 j/7, qui contient les informations les plus récentes sur les problèmes courants et inhabituels pouvant être rencontrés.

Procédure

1. Accédez au site http://esupport.trendmicro.com.
2. Sélectionnez un produit ou un service dans la liste déroulante appropriée, puis indiquez toute autre information associée nécessaire.

   La page **Technical Support** (Assistance technique) du produit s'affiche.
3. Utilisez la zone **Search Support** (Lancer une recherche dans les ressources d'assistance) pour rechercher les solutions disponibles.
4. Si vous ne trouvez aucune solution, cliquez sur **Submit a Support Case** (Envoyer une demande d'assistance) dans le volet de navigation de gauche et fournissez tous les détails nécessaires. Vous avez également la possibilité de soumettre une demande d'assistance via le site ci-dessous :

   http://esupport.trendmicro.com/srf/SRFMain.aspx

Un technicien d'assistance de Trend Micro étudiera votre demande et y répondra sous 24 heures.

Communauté « Security Intelligence »

Les experts en cyber-sécurité de Trend Micro constituent une équipe spécialisée dans la sécurité dans les domaines suivants : détection et analyse des menaces, sécurité en ligne et dans les environnements virtualisés, chiffrement des données.

Rendez-vous sur le site http://www.trendmicro.com/us/security-intelligence/index.html pour en savoir plus sur les sujets suivants :

- Blogs, comptes Twitter et Facebook, chaîne YouTube et autres sites de présence de Trend Micro sur les réseaux sociaux.
- Rapports de menaces, études et articles.
- Solutions, podcasts et newsletters des acteurs principaux de la sécurité à l'échelle mondiale.
- Outils, applications et widgets gratuits.

Encyclopédie des menaces

De nos jours, la plupart des programmes malveillants présentent des « menaces combinées », à savoir deux technologies (ou plus), combinées pour parvenir à contourner les protocoles de sécurité des ordinateurs. Trend Micro combat ces programmes malveillants complexes à l'aide de produits capables de générer une stratégie de défense personnalisée. L'encyclopédie des menaces fournit une liste aussi exhaustive que possible des noms et des symptômes de diverses menaces combinées connues, telles que programmes malveillants, spam, URL malveillantes et vulnérabilités connues.

Rendez-vous sur le site http://about-threats.trendmicro.com/fr/threatencyclopedia#malware pour en savoir plus sur les sujets suivants :

- Programmes malveillants et codes mobiles malveillants actuellement actifs ou « en circulation ».

- Pages d'informations connexes dédiées aux menaces, présentant l'historique complet d'une attaque Web.
- Avis relatifs aux menaces Internet, dédiés à des attaques et à des menaces de sécurité ciblées.
- Informations sur les tendances en matière d'attaques Web.
- Rapports hebdomadaires sur les programmes malveillants.

Comment contacter Trend Micro

Aux États-Unis, les techniciens de Trend Micro peuvent être contactés par téléphone, fax ou courrier électronique :

Adresse	TREND MICRO INCORPORATED Trend Micro SA 85, avenue Albert 1er 92500 Rueil Malmaison France
Téléphone	+33 (0) 1 76 68 65 00
Site Web	http://www.trendmicro.com
Adresse électronique	sales@trendmicro.fr

- Sites d'assistance à travers le monde :

  http://www.trendmicro.fr/apropos/contact/index.html
- Documentation des produits Trend Micro :

  http://docs.trendmicro.com/fr-fr/home.aspx

Accélération du traitement de votre demande d'assistance

Afin d'améliorer la résolution des problèmes, ayez les informations ci-dessous à portée de main :

- Étapes permettant de reproduire le problème

- Informations sur l'appareil et le réseau
- Marque et modèle de l'ordinateur, ainsi que de tout matériel supplémentaire connecté au endpoint
- Quantité de mémoire et d'espace disque disponibles
- Nom et version (Service Pack inclus) du système d'exploitation
- Version du client du endpoint
- Numéro de série ou code d'activation
- Description détaillée de l'environnement d'installation
- Texte exact du message d'erreur affiché

Envoi de contenu suspect à Trend Micro

Plusieurs façons d'envoyer du contenu suspect à Trend Micro pour une analyse plus poussée sont à votre disposition.

Services de File Reputation

Collectez des informations système et envoyez le contenu de fichiers suspects à Trend Micro :

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

Notez le numéro de dossier à des fins de suivi.

services de réputation de messagerie (Email Reputation Services)

Lancez une interrogation de la réputation d'une adresse IP spécifique et indiquez un agent de transfert de messages à inclure dans la liste globale des éléments approuvés :

https://ers.trendmicro.com/

Reportez-vous à l'entrée suivante de la Base de connaissances pour envoyer des échantillons de messages à Trend Micro :

http://esupport.trendmicro.com/solution/en-us/1055473.aspx

Services de réputation de sites Web

Lancez une interrogation de l'évaluation de sécurité et du type de contenu d'une URL que vous pensez correspondre à un site de phishing ou un autre « vecteur de menaces » (source de menaces Internet intentionnelles telles que les spywares et programmes malveillants) :

http://global.sitesafety.trendmicro.com/

Si l'évaluation attribuée est incorrecte, envoyez une demande de reclassification à Trend Micro.

Other Resources

Outre les solutions et l'assistance disponibles en ligne, d'autres ressources, dont le but est de maintenir à jour vos systèmes, de vous informer des innovations les plus récentes et de vous faire connaître les dernières tendances en matière de sécurité, sont également consultables.

TrendEdge

Obtenez des informations sur les techniques novatrices non prises en charge, les outils et les bonnes pratiques liés aux produits et services Trend Micro. La base de données TrendEdge contient de nombreux documents couvrant un large éventail de sujets destinés aux employés et partenaires de Trend Micro, ainsi qu'aux autres parties intéressées.

Consultez les informations les plus récemment ajoutées à TrendEdge à l'adresse :

http://trendedge.trendmicro.com/

Centre de téléchargement

Trend Micro est susceptible de publier, de temps à autre, un patch corrigeant un problème connu ou une mise à niveau s'appliquant à un produit ou service particulier. Pour savoir si des patches sont disponibles, rendez-vous sur le site :

http://downloadcenter.trendmicro.com/index.php?regs=fr

Si l'un des patches disponibles n'a pas été appliqué (les patches sont datés), ouvrez le fichier Lisez-moi afin de déterminer s'il convient à votre environnement. Le fichier Lisez-moi contient également des instructions d'installation.

TrendLabs

TrendLabs℠ est un réseau mondial de centres de recherche, de développement et d'action dédiés à la surveillance des menaces, à la prévention des attaques et à la publication rapide et transparente de solutions 24 h/24 et 7 j/7. Véritable clef de voûte de l'infrastructure de services de Trend Micro, l'équipe de TrendLabs se compose de plusieurs centaines de techniciens et d'employés certifiés qui proposent un large éventail de services d'assistance technique et d'assistance produit.

TrendLabs surveille l'apparition et l'évolution des menaces à l'échelle mondiale, afin de pouvoir proposer des mesures de sécurité efficaces permettant de détecter, de bloquer et d'éliminer les attaques. La portée de ces efforts se mesure au jour le jour, par le biais des mises à jour des fichiers de signatures de virus et des ajustements apportés au moteur de scan fréquemment transmis à nos clients.

Pour en savoir plus sur TrendLabs, rendez-vous sur le site :

http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs

Annexes





Annexe A

Prise en charge de l'adressage IPv6 dans OfficeScan

Cette annexe doit être lue par les utilisateurs qui prévoient de déployer OfficeScan dans un environnement prenant en charge l'adressage IPv6. Cette annexe contient des informations sur le degré de prise en charge d'IPv6 dans OfficeScan.

Trend Micro suppose que le lecteur est familiarisé avec les concepts d'IPv6 et les tâches qu'implique la configuration d'un réseau prenant en charge l'adressage IPv6.

Prise en charge de l'adressage IPv6 pour le serveur et les agents OfficeScan

Cette version 10.6 est la première à prendre en charge l'adressage IPv6 pour OfficeScan. Les versions précédentes de OfficeScan ne prennent pas en charge l'adressage IPv6. La prise en charge de l'adressage IPv6 est automatiquement activée après l'installation ou la mise à niveau du serveur OfficeScan et des agents OfficeScan répondant aux exigences de l'adressage IPv6.

Configuration requise pour le serveur OfficeScan

Les exigences IPv6 pour le serveur OfficeScan sont les suivantes :

- Le serveur doit être installé sur Windows Server 2008 ou Windows Server 2012. Il ne peut pas être installé sur Windows Server 2003, car ce système d'exploitation ne prend que partiellement en charge l'adressage IPv6.
- Le serveur doit utiliser un serveur Web IIS. Le serveur Web Apache ne prend pas en charge l'adressage IPv6.
- Si le serveur peut gérer des agents OfficeScan IPv4 et IPv6, il doit disposer d'adresses IPv4 et IPv6 et doit être identifié par son nom d'hôte. Si un serveur est identifié par son adresse IPv4, les agents OfficeScan IPv6 ne peuvent pas s'y connecter. Le même problème se pose lorsque des agents IPv4 purs se connectent à un serveur identifié par son adresse IPv6.
- Si le serveur ne gère que des agents IPv6, la configuration minimale requise est une adresse IPv6. Le serveur peut être identifié par son nom d'hôte ou son adresse IPv6. Lorsque le serveur est identifié par son nom d'hôte, il est préférable d'utiliser le nom de domaine complet (FQDN). En effet, dans un environnement exclusivement IPv6, un serveur WINS ne peut pas convertir un nom d'hôte en une adresse IPv6 correspondante.



Remarque

Le nom de domaine complet ne peut être spécifié que lors de l'installation locale du serveur. Il n'est pas pris en charge pour les installations à distance.

Configuration requise pour l'agent OfficeScan

L'agent OfficeScan doit être installé sur :

- Windows 7
- Windows Server 2008
- Windows Vista
- Windows 8
- Windows 8.1
- Windows Server 2012

Il ne peut être installé sur Windows Server 2003 ni Windows XP car ces systèmes d'exploitation ne prennent que partiellement en charge l'adressage IPv6.

Il est préférable qu'un agent OfficeScan possède à la fois une adresse IPv4 et une adresse IPv6, car certaines des entités auxquelles il se connecte ne prennent en charge que l'adressage IPv4.

Limitations des serveurs IPv6 purs

Le tableau suivant répertorie les restrictions pour un serveur OfficeScan possédant uniquement des adresses IPv6.

TABLEAU A-1. Limitations des serveurs IPv6 purs

ÉLÉMENT	RESTRICTION
Gestion des agents	Un serveur IPv6 ne peut : • Déployer des agents OfficeScan sur des endpoints IPv4 purs. • Gérer des agents OfficeScan IPv4 purs.

Élément	Restriction
Mises à jour et gestion centralisée	Un serveur IPv6 pur ne peut effectuer de mises à jour à partir de sources de mise à jour IPv4 pures, telles que : • Trend Micro ActiveUpdate Server • Toute source de mise à jour personnalisée IPv4 pure
Enregistrement, activation et renouvellement du produit	Un serveur IPv6 pur ne peut se connecter au serveur d'enregistrement en ligne de Trend Micro pour enregistrer le produit, obtenir la licence et activer/renouveler la licence.
Connexion Proxy	Un serveur IPv6 pur ne peut se connecter via un serveur proxy IPv4 pur.
Solutions de plug-in	Un serveur IPv6 pur dispose de Plug-in Manager mais ne peut déployer aucune des solutions modules additionnels sur : • Des agents OfficeScan IPv4 purs ou des hôtes IPv4 purs (du fait de l'absence de connexion directe). • Des agents OfficeScan IPv6 purs ou des hôtes IPv6 purs, car aucune des solutions modules additionnels ne prend en charge IPv6.

La plupart de ces restrictions peuvent être surmontées en configurant un serveur proxy à double pile pouvant convertir les adresses IPv4 et IPv6 (tel que DeleGate). Positionnez le serveur proxy entre le serveur OfficeScan et les entités auxquelles il se connecte ou les entités qu'il dessert.

Limitations des agents OfficeScan IPv6 purs

Le tableau suivant répertorie les limitations dont souffrent les agents OfficeScan possédant uniquement des adresses IPv6.

Tableau A-2. Limitations des agents OfficeScan IPv6 purs

Élément	Restriction
Serveur OfficeScan parent	Les agents OfficeScan IPv6 purs ne peuvent pas être gérés par un serveur OfficeScan IPv4 pur.

ÉLÉMENT	RESTRICTION
Mises à jour	Un agent OfficeScan IPv6 pur ne peut pas effectuer de mises à jour à partir de sources de mise à jour IPv4 pures, telles que : • Trend Micro ActiveUpdate Server • un serveur OfficeScan IPv4 pur • un agent de mise à jour IPv4 pur • Toute source de mise à jour personnalisée IPv4 pure
Requêtes de scan, requêtes de réputation de sites Web et Smart Feedback	Un agent OfficeScan IPv6 pur ne peut pas envoyer de requêtes à des sources Smart Protection telles que : • Smart Protection Server 2.0 (intégré ou autonome) **Remarque** IPv6 est pris en charge pour le serveur Smart Protection Server à partir de la version 2.5. • Trend Micro Smart Protection Network (également pour Smart Feedback)
Sécurité des logiciels	Les agents OfficeScan IPv6 purs ne peuvent pas se connecter au service Certified Safe Software Service hébergé par Trend Micro.
Solutions de plug-in	Les agents OfficeScan IPv6 purs ne peuvent pas installer de solutions modules additionnels car aucune de ces solutions ne prend en charge IPv6.
Connexion Proxy	Un agent OfficeScan IPv6 pur ne peut pas se connecter via un serveur proxy IPv4 pur.

La plupart de ces restrictions peuvent être surmontées en configurant un serveur proxy à double pile pouvant convertir les adresses IPv4 et IPv6 (tel que DeleGate). Placez le serveur proxy entre les agents OfficeScan et les entités auxquelles ils se connectent.

Configuration des adresses IPv6

La console Web vous permet de configurer une adresse IPv6 ou une plage d'adresses IPv6. Voici quelques instructions de configuration.

- OfficeScan accepte les présentation d'adresse IPv6 standard.

  Par exemple :

  `2001:0db7:85a3:0000:0000:8a2e:0370:7334`

  `2001:db7:85a3:0:0:8a2e:370:7334`

  `2001:db7:85a3::8a2e:370:7334`

  `::ffff:192.0.2.128`

- OfficeScan accepte également les adresses IPv6 avec un lien local, telles que :

  `fe80::210:5aff:feaa:20a2`



AVERTISSEMENT!

Faites attention lors de la spécification d'une adresse IPv6 avec un lien local car, même si OfficeScan accepte cette adresse, il se peut qu'il ne fonctionne pas comme attendu dans certaines circonstances. Par exemple, les agents OfficeScan ne peuvent pas effectuer de mise à jour à partir d'une source de mise à jour si celle-ci se trouve sur un segment différent du réseau et est identifiée par son adresse IPv6 avec lien local.

- Lorsque l'adresse IPv6 fait partie d'une URL, placez-la entre crochets ([]).
- Pour les plages d'adresses IPv6, un préfixe et une longueur de préfixe sont généralement requis. Pour les configurations qui requièrent que le serveur interroge des adresses IP, des restrictions de longueur de préfixe s'appliquent afin d'empêcher tout problème de performance lorsque le serveur interroge un grand nombre d'adresses IP. Par exemple, pour la fonction de gestion des serveurs externes, la longueur du préfixe doit être comprise entre 112 (65,536 adresses IP) et 128 (2 adresses IP).
- Certains paramètres impliquant des adresses ou des plages d'adresses IPv6 seront déployés pour les agents OfficeScan, mais ces agents OfficeScan n'en auront pas

connaissance. Par exemple, si vous avez configuré la liste des sources Smart Protection et inclus un serveur Smart Protection Server identifié par son adresse IPv6, les agents OfficeScan IPv4 purs ignorent le serveur et se connectent à d'autres sources Smart Protection.

Écrans affichant les adresses IP

Cette rubrique dresse la liste des endroits de la console Web où sont affichées les adresses IP.

- Arborescence des agents

  À chaque fois que l'arborescence des agents s'affiche, les adresses IPv6 des agents OfficeScan IPv6 purs s'affichent dans la colonne **Adresse IP**. Les adresses IPv6 des agents OfficeScan à double pile s'affichent s'ils ont utilisé leur adresse IPv6 pour s'enregistrer auprès du serveur.

  Remarque

  L'adresse IP utilisée par les agents OfficeScan à double pile lors de leur enregistrement auprès du serveur peut être contrôlée dans **Agents** > **Paramètres de l'agent général > Adresse IP de votre choix**.

  Lorsque vous exportez les paramètres de l'arborescence des agents dans un fichier, les adresses IPv6 s'affichent également dans le fichier exporté.

- État de l'agent

  Des informations détaillées sur les agents sont disponibles lorsque vous accédez à **Agents** > **Gestion des agents > État**. Sur cet écran sont affichées les adresses IPv6 des agents OfficeScan IPv6 purs et des agents OfficeScan à double pile ayant utilisé leurs adresses IPv6 pour s'enregistrer auprès du serveur.

- Journaux

  Les adresses IPv6 des agents OfficeScan à double pile et IPv6 purs sont présentées dans les journaux suivants :

  - Journaux de virus/programmes malveillants

- Journaux de spywares/graywares
- Journaux de pare-feu
- Journaux de vérification de la connexion

- Console Control Manager

Le tableau suivant répertorie les adresses IP du serveur OfficeScan et des agents OfficeScan s'affichant sur la console Control Manager.

TABLEAU A-3. Adresses IP du serveur OfficeScan et des agents OfficeScan s'affichant sur la console Control Manager

OFFICESCAN	VERSION DE CONTROL MANAGER		
	5.5 SP1	**5.5**	**5.0**
Serveur à double pile	IPv4 et IPv6	IPv4	IPv4
Serveur IPv4 pur	IPv4	IPv4	IPv4
Serveur IPv6 pur	IPv6	Non pris en charge	Non pris en charge
Agent OfficeScan à double pile	Adresse IP utilisée lors de l'enregistrement de l'agent OfficeScan auprès du serveur OfficeScan	Adresse IP utilisée lors de l'enregistrement de l'agent OfficeScan auprès du serveur OfficeScan	Adresse IP utilisée lors de l'enregistrement de l'agent OfficeScan auprès du serveur OfficeScan
Agent OfficeScan IPv4 pur	IPv4	IPv4	IPv4
Agent OfficeScan IPv6 pur	IPv6	IPv6	IPv6



Annexe B

Prise en charge de Windows Server Core 2008/2012

Cette annexe présente la prise en charge par OfficeScan de Windows Server Core 2008/2012.

Prise en charge de Windows Server Core 2008/2012

Windows Server Core 2008/2012 est une installation minimale de Windows Server 2008/2012. Dans un environnement Server Core :

- De nombreuses options et fonctionnalités de Windows Server 2008/2012 sont supprimées.
- Le système exécute un système d'exploitation central beaucoup plus léger.
- Les tâches sont effectuées principalement depuis l'interface de ligne de commande.
- Le système d'exploitation exécute moins de services et nécessite moins de ressources au démarrage.

L'agent OfficeScan prend en charge Server Core. Cette section contient des informations sur l'étendue de la prise en charge de Server Core.

Le serveur OfficeScan ne prend pas en charge Server Core.

Méthodes d'installation de Windows Server Core

Les méthodes d'installation suivantes ne sont pas prises en charge, ou le sont uniquement en partie :

- Page Web d'installation : cette méthode n'est pas prise en charge car Server Core ne dispose pas d'Internet Explorer.
- Trend Micro Vulnerability Scanner : l'outil Vulnerability Scanner ne peut pas être exécuté localement sur Server Core. Exécutez l'outil depuis le serveur OfficeScan ou un autre endpoint.

Les méthodes d'installation suivantes sont prises en charge :

- Installation à distance. Pour obtenir des informations détaillées, voir *Installation à distance depuis OfficeScan Web Console à la page 5-20*.

- Configuration du script de connexion
- Agent Packager

Installation de l'agent OfficeScan à l'aide de l'outil Configuration du script de connexion

Procédure

1. Ouvrez une invite de commande.
2. Mappez l'emplacement du fichier `AutoPcc.exe` en entrant la commande suivante :

```
net use <lettre du lecteur mappé> \\<nom d'hôte ou adresse IP du serveur OfficeScan>\ofcscan
```

Par exemple :

```
net use P : \\10.1.1.1\ofcscan
```

Un message s'affiche, vous informant que l'emplacement du fichier `AutoPcc.exe` a été mappé.

3. Accédez à l'emplacement du fichier `AutoPcc.exe` en indiquant la lettre du lecteur mappé suivie de deux points (:). Par exemple :

```
P:
```

4. Entrez ce qui suit pour démarrer l'installation :

```
AutoPcc.exe
```

L'écran ci-dessous montre les commandes et les résultats de l'invite de commande.

```
c:\Windows>net use P: \\172.16.9.61\ofcscan
La commande s'est terminée correctement.


c:\Windows>P:

P:\>AutoPcc.exe
AutoPcc.exe

|-------------------------------------------------|
|        Trend Micro OfficeScan                   |
|       Programme d'installation automatique V11.0 |
|      Copyright Trend Micro, Inc.                |
|              1998-2014                          |
|-------------------------------------------------|

P:\>
```

FIGURE B-1. Invite de commandes indiquant comment installer l'agent OfficeScan à l'aide de l'outil Configuration du script de connexion

Installation de l'agent OfficeScan à l'aide du package de l'agent OfficeScan

Procédure

1. Créez le pack.

   Pour obtenir des informations détaillées, voir *Installation à l'aide de l'outil Agent Packager à la page 5-26*.

2. Ouvrez une invite de commande.

3. Mappez l'emplacement du package de l'agent OfficeScan en saisissant la commande suivante :

```
net use <lettre du lecteur mappé> \\<Emplacement du package de l'agent>
```

   Par exemple :

```
net use P : \\10.1.1.1\Package
```

Un message s'affiche, vous informant que l'emplacement du package de l'agent OfficeScan a été mappé.

4. Remplacez le répertoire existant par l'emplacement du package de l'agent OfficeScan en saisissant la lettre du lecteur mappé suivie de deux points. Par exemple :

```
P:
```

5. Copiez le package de l'agent OfficeScan dans un répertoire local du endpoint Server Core en saisissant la commande suivante :

```
copy <nom du fichier du package> <répertoire du endpoint
Server Core où vous souhaitez copier le package>
```

Par exemple :

```
copy officescan.msi C:\Client Package
```

Un message s'affiche, vous informant que le package de l'agent OfficeScan a été copié.

6. Accédez au répertoire local. Par exemple :

```
C:
```

```
cd C:\Client Package
```

7. Entrez le nom du fichier de pack pour démarrer l'installation. Par exemple :

```
officescan.msi
```

L'écran ci-dessous montre les commandes et les résultats de l'invite de commande.

```
C:\Windows>net use P: \\172.16.9.61\Package
La commande s'est terminée correctement.

C:\Windows>P:

P:\>copy officescan.msi "C:\Client Package"
        1 fichier(s) copié(s).

P:\>c:

C:\Windows>cd "C:\Client Package"

C:\Client Package>officescan.msi
```

FIGURE B-2. Invite de commandes indiquant comment installer l'agent OfficeScan à l'aide d'un package agent

Fonctionnalités de l'agent OfficeScan sur Windows Server Core

La plupart des fonctionnalités de l'agent OfficeScan disponibles sur Windows Server 2008/2012 fonctionnent sur Server Core. La seule fonctionnalité non prise en charge est le mode itinérance.

Pour obtenir une liste des fonctionnalités disponibles sur Windows Server 2008/2012, voir *Fonctionnalités de l'agent OfficeScan à la page 5-3*.

La console de l'agent OfficeScan n'est accessible que depuis l'interface de ligne de commande.



Remarque

Certains écrans de la console de l'agent OfficeScan contiennent un bouton Aide, sur lequel vous pouvez cliquer pour afficher une aide HTML contextuelle. Étant donné que Windows Server Core 2008/2012 ne contient pas de navigateur, l'utilisateur ne pourra pas accéder à l'aide. Pour y avoir accès, l'utilisateur doit installer un navigateur.

Commandes Windows Server Core

Lancez la console de l'agent OfficeScan et d'autres tâches de l'agent OfficeScan en saisissant des commandes dans l'interface de ligne de commande.

Pour exécuter les commandes, accédez à l'emplacement de `PccNTMon.exe`. Ce processus est responsable du lancement de la console de l'agent OfficeScan. Vous le trouverez dans le <*dossier d'installation de l'agent*>.

Le tableau suivant répertorie les commandes disponibles.

Tableau B-1. Commandes Windows Server Core

Commande	Action
pccntmon	Ouvre la console de l'agent OfficeScan.
pccnt	
pccnt <lecteur ou chemin d'accès du dossier>	Effectue un scan du lecteur ou du dossier spécifié pour vérifier les risques de sécurité Directives : • Si le chemin d'accès du dossier contient un espace, mettez le chemin complet entre guillemets. • Il est impossible d'effectuer un scan de fichiers individuels. Commandes correctes : • pccnt C:\ • pccnt D:\Files • pccnt « C:\Documents and Settings » Commandes incorrectes : • pccnt C:\Documents and Settings • pccnt D:\Files\example.doc
pccntmon -r	Ouvre la surveillance en temps réel
pccntmon -v	Ouvre un écran répertoriant les composants de l'agent et leur version.

COMMANDE	ACTION
`pccntmon -u`	Ouvre un écran dans lequel vous pouvez lancer la commande « Mettre à jour » (mise à jour manuelle de l'agent). Si « Mettre à jour » ne peut pas être lancé, le message suivant s'affiche dans l'invite de commande : Désactivé ou Non opérationnel
`pccntmon -n`	Ouvre une fenêtre contextuelle contenant le mot de passe de déchargement de l'agent. Si aucun mot de passe n'est nécessaire pour décharger l'agent OfficeScan, le déchargement de l'agent OfficeScan commence. Pour recharger l'agent OfficeScan, saisissez la commande suivante : `pccntmon`
`pccntmon -m`	Ouvre une fenêtre contextuelle contenant le mot de passe de désinstallation de l'agent OfficeScan. Si aucun mot de passe n'est nécessaire pour désinstaller l'agent OfficeScan, la désinstallation de l'agent OfficeScan commence.

COMMANDE	ACTION
`pccntmon -c`	Affiche les informations suivantes dans la ligne de commande : • Méthode de scan • Smart scan • Scan traditionnel • État des signatures • Mis à jour • Obsolète • service de scan en temps réel • Opérationnel • Désactivé ou Non opérationnel • État de la connexion de l'agent • En ligne • Itinérant • Hors ligne • Services de réputation de sites Web • Disponible • Reconnexion • Services de File Reputation • Disponible • Reconnexion
`pccntmon -h`	Affiche toutes les commandes disponibles



Annexe C

Prise en charge de Windows 8/8.1 et Windows Server 2012

Cette annexe présente la prise en charge d'OfficeScan sous Windows 8/8.1 et Windows Server 2012.

À propos de Windows 8/8.1 et Windows Server 2012

Windows 8/8.1 et Windows Server 2012 offrent aux utilisateurs deux types de mode de fonctionnement : le mode Poste de travail et le mode Windows UI. Le mode Poste de travail est similaire à l'écran classique **Démarrer** de Windows.

Le mode Windows UI propose aux utilisateurs une nouvelle interface utilisateur, similaire à celle employée dans les Windows phones. Parmi les nouvelles fonctionnalités, on retrouve une interface tactile déroulante, des vignettes et des notifications toast.

TABLEAU C-1. Vignettes et notifications toast

CONTRÔLE	DESCRIPTION
Vignettes	Les vignettes sont similaires aux icônes du poste de travail des versions précédentes de Windows. Les utilisateurs cliquent ou appuient sur une vignette pour démarrer l'application qui lui est associée. Les vignettes dynamiques offrent aux utilisateurs des informations propres aux applications qui se mettent à jour de manière dynamique. Les applications peuvent publier des informations sur les vignettes, même lorsque l'application n'est pas en cours d'exécution.
Notifications toast	Les notifications toast sont similaires aux messages contextuels. Ces notifications fournissent des informations sensibles quant au temps sur les événements qui se produisent pendant l'exécution d'une application. Les notifications apparaissent à l'avant-plan, que Windows soit en mode Poste de travail, affiche l'écran de verrouillage ou soit en train d'exécuter une autre application. **Remarque** En fonction de l'application, les notifications toast peuvent ne pas apparaître sur tous les écrans ou dans tous les modes.

OfficeScan en mode Windows UI

Le tableau suivant décrit comment OfficeScan prend en charge les vignettes et les notifications toast en mode Windows UI.

TABLEAU C-2. Prise en charge par OfficeScan des vignettes et notifications toast

CONTRÔLE	PRISE EN CHARGE PAR OFFICESCAN
Vignettes	OfficeScan fournit aux utilisateurs une vignette qui les renvoie vers le programme de l'agent OfficeScan. Lorsque les utilisateurs cliquent sur cette vignette, Windows bascule en mode Poste de travail et le programme de l'agent OfficeScan s'affiche. **Remarque** OfficeScan ne prend pas en charge les vignettes dynamiques.
Notifications toast	OfficeScan fournit les notifications toast suivantes : • Programme suspect détecté • Scan programmé • Menaces résolues • Redémarrage de l'ordinateur requis • Périphérique de stockage USB détecté • Épidémie détectée **Remarque** OfficeScan n'affiche les notifications toast qu'en mode Windows UI.

Activation des notifications toast

Les utilisateurs peuvent choisir de recevoir des notifications toast en modifiant les **Paramètres du PC** du endpoint de l'agent OfficeScan. OfficeScan requiert l'activation des notifications toast par l'utilisateur.

Procédure

1. Déplacez le curseur de la souris dans le coin inférieur droit de l'écran pour afficher la barre des **Symboles**.

2. Cliquez sur **Paramètres** > **Modifier les paramètres du PC**.

   L'écran **Paramètres du PC** apparaît.

3. Cliquez sur **Notifications**.

4. Dans la section **Notifications**, définissez les paramètres suivants sur **Activé** :

   - **Afficher les notifications d'application**
   - **Afficher les notifications d'application sur l'écran de verrouillage** (facultatif)
   - **Lire les sons de notification** (facultatif)

Internet Explorer 10/11

Internet Explorer (IE) 10 est le navigateur par défaut sous Windows 8/8.1 et Windows Server 2012. Il est fourni en deux versions distinctes : une pour le mode Windows UI et l'autre pour le mode Bureau.

Internet Explorer 10 et versions ultérieures pour Windows UI offre une navigation sans module additionnel. Les modules additionnels de navigation Internet ne répondant à aucune norme, la qualité du code qu'ils emploient est donc variable. Ils nécessitent en outre plus de ressources système et augmentent le risque d'infection par des programmes malveillants.

Microsoft a développé Internet Explorer 10 et versions ultérieures pour Windows UI afin de suivre des technologies basées sur de nouvelles normes et remplacer les modules additionnels précédemment utilisés. Le tableau suivant répertorie les technologies utilisées par Internet Explorer 10 et versions ultérieures à la place de l'ancienne technologie module additionnelle.

Tableau C-3. Comparaison entre les technologies basées sur les normes et les modules additionnels

Fonctionnalités	Technologie standard du World Wide Web (W3C)	Exemple en équivalent module additionnel
Vidéo et audio	Vidéo et audio HTML5	• Flash • Apple QuickTime • Silverlight
Graphiques	• Canvas HTML5 • Scalable Vector Graphics (SVG) • Feuilles de style en cascade, niveau 3 (CSS3) Transitions et animations • Transformations CSS	• Flash • Apple QuickTime • Silverlight • Applets java
Stockage hors ligne	• Stockage sur le Web • Fichier API • IndexedDB • API application cache	• Flash • Applets java • Google Gears
Communication réseau, partage des ressources, chargement de fichier	• Messagerie Web HTML • Technologie CORS (Cross-origin resource sharing)	• Flash • Applets java

Microsoft a également développé une version d'Internet Explorer 10 et versions ultérieures compatible avec les modules additionnels, uniquement pour le mode Bureau. Si les utilisateurs du mode Windows UI trouvent un site Web qui nécessite l'utilisation de modules additionnels supplémentaires, une notification s'affiche dans Internet Explorer 10 et versions ultérieures, invitant les utilisateurs à basculer en mode Bureau. Lorsque les utilisateurs basculent en mode Bureau, ils peuvent voir les sites Web qui nécessitent l'utilisation ou l'installation de modules additionnels tiers.

Prise en charge des fonctionnalités d'OfficeScan dans Internet Explorer 10/11

Le mode d'exécution de Windows 8/8.1 ou Windows Server 2012 a un impact sur la version d'Internet Explorer 10 et versions ultérieures, et donc sur la prise en charge des différentes fonctionnalités d'OfficeScan. Le tableau suivant répertorie les niveaux de prise en charge pour les fonctionnalités d'OfficeScan en mode Poste de travail et Windows UI.



Remarque

Les fonctionnalités qui ne sont pas reprises dans le tableau prennent en charge les deux modes de fonctionnement.

Tableau C-4. Prise en charge des fonctions OfficeScan en mode Windows UI

Fonction	Mode Poste de travail	Windows UI
Console Web du serveur	Prise en charge totale	Non pris en charge
Réputation de sites Web	Prise en charge totale	Prise en charge partielle • Scan HTTPS désactivé
Pare-feu	Prise en charge totale	Prise en charge partielle • Filtrage des applications désactivé



Annexe D

Rétrogradation d'OfficeScan

Cette annexe présente la prise en charge de la rétrogradation du serveur et des agents OfficeScan.

Rétrogradation du serveur et des agents OfficeScan

La procédure de rétrogradation d'OfficeScan implique dans un premier temps la rétrogradation des agents OfficeScan, puis celle du serveur OfficeScan dans un second.



Important

- Les administrateurs ne peuvent procéder à la rétrogradation du serveur et des agents OfficeScan à l'aide de la procédure suivante que si l'administrateur en charge du processus d'installation a choisi de sauvegarder le serveur. Si aucun fichier de sauvegarde du serveur n'est disponible, consultez les procédures manuelles de rétrogradation dans le *Guide d'installation et de mise à niveau* pour la version précédemment installée d'OfficeScan.
- Cette version d'OfficeScan prend uniquement en charge la rétrogradation à partir des versions suivantes :
    - OfficeScan 10.6 (y compris toutes les versions des Service Packs)
    - OfficeScan 10.5
    - OfficeScan 10.0

Rétrogradation des agents OfficeScan

OfficeScan ne peut rétrograder des agents OfficeScan que vers la version du serveur subissant une restauration. Il est impossible de rétrograder des agents OfficeScan vers une version antérieure à celle du serveur.



Important

Assurez-vous de rétrograder les agents OfficeScan avant de procéder à la rétrogradation du serveur OfficeScan.

Procédure

1. Assurez-vous que les agents OfficeScan peuvent procéder à la mise à niveau de leur programme.

a. Sur la console Web OfficeScan 11.0, accédez à **Agents** > **Gestion des agents**.

b. Sélectionnez les agents OfficeScan à rétrograder.

c. Cliquez sur l'onglet **Paramètres** > **Privilèges et autres paramètres** > **Autres paramètres**.

d. Activez l'option **Les agents OfficeScan peuvent mettre à jour les composants, mais ne peuvent pas mettre à niveau le programme de l'agent, ni déployer des correctifs de type hot fix**.

2. Sur la console Web OfficeScan 11.0, accédez à **Mises à jour** > **Agents** > **Source de mise à jour**.

3. Sélectionnez **Source de mise à jour personnalisée**.

4. Dans la liste **Liste des sources de mise à jour personnalisée**, cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.

5. Saisissez les adresses IP des agents OfficeScan à rétrograder.

6. Entrez l'URL de la source de mise à jour.

   Par exemple, entrez :

```
http://<adresse IP du serveur OfficeScan>:<port>/
OfficeScan/download/Rollback
```

7. Cliquez sur **Enregistrer**.

8. Cliquez sur **Notifier tous les agents**.

   Lorsque l'agent OfficeScan devant être rétrogradé se met à jour à partir de la source de mise à jour, il est désinstallé et la version précédente de l'agent est installée.



Conseil

Les administrateurs peuvent accélérer le processus de rétrogradation en lançant une mise à jour manuelle sur les agents OfficeScan. Pour obtenir des informations détaillées, consultez la section *Mise à jour manuelle des agents OfficeScan à la page 6-49*.

---

9. Une fois la version précédente de l'agent OfficeScan installée, informez l'utilisateur qu'il doit redémarrer l'ordinateur.

   Une fois le processus de rétrogradation effectué, l'agent OfficeScan continue à dépendre du même serveur OfficeScan.

   Remarque

   Une fois la rétrogradation de l'agent OfficeScan effectuée, tous les composants, y compris le fichier de signatures de virus, subissent également une rétrogradation vers leur version précédente. Si les administrateurs n'effectuent pas la rétrogradation du serveur OfficeScan, l'agent OfficeScan ayant subi une rétrogradation ne peut pas mettre à jour ses composants. Les administrateurs doivent rétablir la source de mise à jour standard sur l'agent OfficeScan ayant subi une rétrogradation afin de rendre possible la mise à jour des composants.

Rétrogradation du serveur OfficeScan

La procédure de rétrogradation du serveur OfficeScan nécessite que l'administrateur arrête manuellement les services Windows, mette à jour le Registre système et remplace les fichiers du serveur OfficeScan dans le répertoire d'installation d'OfficeScan.



Important

Assurez-vous de rétrograder les agents OfficeScan avant de procéder à la rétrogradation du serveur OfficeScan.

Procédure

1. Sur l'ordinateur du serveur OfficeScan, arrêtez les services suivants :

   - Intrusion Defense Firewall (si installé)
   - Trend Micro Local Web Classification Server
   - Trend Micro Smart Scan Server
   - Service d'intégration d'Active Directory OfficeScan
   - Agent Control Manager d'OfficeScan

- OfficeScan Plug-in Manager
- Service principal d'OfficeScan
- Apache 2 (si vous utilisez le serveur Web Apache)
- World Wide Web Publishing Service (si vous utilisez le serveur Web IIS)

2. Copiez et remplacez tous les fichiers et dossiers du répertoire <*dossier d'installation du serveur*>`\PCCSRV\Download\Rollback\` vers le répertoire <*dossier d'installation du serveur*>`\PCCSRV\Download\`.

3. Cliquez sur **Démarrer**, tapez `regedit`, puis appuyez sur Entrée.

   L'écran **Éditeur du Registre** s'affiche.

4. Dans le volet de navigation de gauche, sélectionnez l'une des clés de Registre suivantes :

   - Pour les systèmes 32 bits : `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service`
   - Pour les systèmes 64 bits : `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\Officescan\service`

5. Accédez à **Fichier** > **Importer...**.

6. Sélectionnez le fichier `.reg` qui se trouve dans le répertoire <*dossier d'installation du serveur*>`\PCCSRV\Download\Rollback\`.

7. Cliquez sur **Oui** pour restaurer les versions précédentes de toutes les clés d'OfficeScan.

8. Ouvrez un éditeur de ligne de commande (cliquez sur **Démarrer** et tapez `cmd.exe`), puis entrez les commandes suivantes afin de réinitialiser le compteur de performances du serveur Local Web Classification Server :

```
cd <dossier d'installation du serveur>\PCCSRV\LWCS

regsvr32.exe /u /s perfLWCSPerfMonMgr.dll

regsvr32.exe /s perfLWCSPerfMonMgr.dll
```

9. Redémarrez les services suivants :

- Intrusion Defense Firewall (si installé)
- Trend Micro Local Web Classification Server
- Trend Micro Smart Scan Server
- Service d'intégration d'Active Directory OfficeScan
- Agent Control Manager d'OfficeScan
- OfficeScan Plug-in Manager
- Service principal d'OfficeScan
- Apache 2 (si vous utilisez le serveur Web Apache)
- World Wide Web Publishing Service (si vous utilisez le serveur Web IIS)

10. Nettoyez le cache d'Internet Explorer et supprimez manuellement les contrôles ActiveX. Pour obtenir des instructions détaillées sur la suppression des contrôles ActiveX d'Internet Explorer 9, consultez la page http://windows.microsoft.com/en-us/internet-explorer/manage-add-ons#ie=ie-9.

La version précédemment installée du serveur OfficeScan a été restaurée.



Conseil

Les administrateurs peuvent confirmer la réussite de la rétrogradation en vérifiant le numéro de version d'OfficeScan sur l'écran **À propos de** (**Aide** > **À propos de**).

11. Une fois la réussite de la rétrogradation d'OfficeScan confirmée, supprimez tous les fichiers qui se trouvent dans le répertoire <dossier_installation_serveur>\PCCSRV\Download\Rollback\.



Annexe E

glossaire

Les termes contenus dans ce glossaire fournissent des d'informations complémentaires sur les termes informatiques couramment référencés, ainsi que sur les produits et technologies Trend Micro.

ActiveUpdate

ActiveUpdate est une fonction commune à de nombreux produits Trend Micro. Connecté au site Web de mises à jour de Trend Micro, ActiveUpdate propose des téléchargements à jour de fichiers de signatures de virus, moteurs de scan, programmes et autres fichiers de composants Trend Micro via Internet.

Fichier compressé

Fichier unique contenant un ou plusieurs fichiers distincts ainsi que des informations leur permettant d'être extraits par un programme approprié, tel que WinZip.

Cookie

Mécanisme permettant de stocker des informations sur un utilisateur d'Internet, telles que son nom, ses préférences et ses centres d'intérêt, qui sont enregistrées dans le navigateur Web pour une utilisation ultérieure. La prochaine fois que vous accéderez à un site Web pour lequel votre navigateur dispose d'un cookie, le navigateur l'enverra au serveur Web et ce dernier pourra l'utiliser pour vous présenter des pages Web personnalisées. Par exemple, vous pouvez accéder à un site Web qui vous accueille en mentionnant votre nom.

Refus de service (DoS)

Le déni de service (DoS) est une attaque affectant un endpoint ou un réseau et entraînant une perte du « service », c'est-à-dire de la connexion réseau. En général, les attaques de déni de service ont une incidence négative sur la bande passante du réseau ou surchargent les ressources système, telles que la mémoire du endpoint.

DHCP

Dynamic Host Control Protocol (DHCP) est un protocole permettant d'affecter des adresses IP dynamiques aux dispositifs d'un réseau. Avec l'adressage dynamique, un dispositif peut avoir une adresse différente chaque fois qu'il se connecte au réseau. Sur certains systèmes, l'adresse IP du dispositif peut même changer alors qu'il est encore connecté. DHCP prend également en charge une combinaison d'adresses IP statiques et dynamiques.

DNS

Domain Name system (DNS) est un service à usage général d'interrogation de données servant principalement sur Internet à convertir les noms d'hôtes en adresses IP.

Lorsqu'un agent DNS demande les données de nom d'hôte et d'adresse à un serveur DNS, le processus s'appelle résolution. Avec la configuration DNS de base, un serveur effectue une résolution par défaut. Par exemple, un serveur distant interroge un autre serveur pour obtenir les données figurant sur un ordinateur dans la zone actuelle. Le logiciel de l'agent sur le serveur distant interroge le résolveur, qui répond à la demande à partir de ses fichiers de base de données.

Nom de domaine

Nom complet d'un système, composé du nom d'hôte local et du nom de domaine correspondants, par exemple `tellsitall.com`. Un nom de domaine doit permettre de déterminer une adresse Internet unique pour tout hôte présent sur Internet. Ce processus, appelé « résolution de nom », utilise le système DNS (Domain Name System).

Adresse IP dynamique

Une adresse IP dynamique est une adresse IP attribuée par un serveur DHCP. L'adresse MAC du endpoint reste la même ; toutefois, le serveur DHCP peut attribuer une nouvelle adresse IP au endpoint, en fonction de la disponibilité.

ESMTP

ESMTP (Enhanced Simple Mail Transport Protocol) inclut la sécurité, l'authentification et d'autres dispositifs pour économiser la bande passante et protéger les serveurs.

Contrat de licence utilisateur final

Un contrat de licence utilisateur final ou CLUF est un contrat légal passé entre un éditeur de programme et l'utilisateur final. Il décrit généralement les restrictions s'appliquant à l'utilisateur, qui peut refuser de conclure l'accord en ne cliquant pas sur «J'accepte» au cours de l'installation. En cliquant sur «Je n'accepte pas», l'utilisateur mettra évidemment fin à l'installation du produit logiciel.

De nombreux utilisateurs acceptent par inadvertance d'installer un spyware et d'autres types de grayware sur leur ordinateur lorsqu'ils cliquent sur «J'accepte» sur des invites du CLUF s'affichant lors de l'installation de certains programmes gratuits.

Faux positif

On parle de faux positif lorsqu'un fichier est considéré à tort comme un fichier infecté par le logiciel de sécurité.

FTP

FTP (File Transfer Protocol) est un protocole standard utilisé pour transférer des fichiers d'un serveur vers un client via Internet. Consultez Network Working Group RFC 959 pour de plus amples informations.

GeneriClean

GeneriClean, programme aussi connu sous le nom de nettoyage référentiel, constitue une nouvelle technologie de nettoyage des virus/programmes malveillants qui ne nécessite pas de composants de nettoyage de virus. En utilisant un fichier détecté comme référence, GeneriClean détermine si le fichier détecté présente un processus/service correspondant dans la mémoire et une entrée de registre, puis supprime tous ces éléments.

Correctif de type hotfix

Un correctif de type Hot Fix désigne une solution palliative à un problème spécifique signalé par un utilisateur. Les correctifs de type hotfix sont spécifiques aux problèmes et ne sont dès lors pas proposés à tous les clients. Les correctifs de types hotfix Windows comprennent un programme d'installation. Ce n'est pas le cas des correctifs de types hotfix qui ne sont pas issus de Windows (en général, vous devez arrêter les démons du programme, copier le fichier pour écraser son équivalent dans votre installation, puis redémarrer les démons).

Par défaut, les agents OfficeScan peuvent installer des correctifs de type hot fix. Si vous ne voulez pas que les agents OfficeScan installent ce type de correctifs, modifiez les paramètres de mise à jour de l'agent dans la console Web en accédant à **Agents** > **Gestion des agents**, cliquez sur l'onglet **Paramètres** > **Privilèges et autres paramètres** > **Autres paramètres**.

Si vous ne parvenez pas à déployer un correctif de type hotfix sur le serveur OfficeScan, utilisez Touch Tool pour changer l'horodatage du correctif de type hotfix. OfficeScan considère alors qu'il s'agit d'un nouveau correctif de type hotfix, ce qui amène le serveur à tenter automatiquement un nouveau déploiement du correctif. Pour plus de détails sur

cet outil, consultez *Exécution de l'outil Touch Tool pour les correctifs de type hot fix des agents OfficeScan à la page 6-58*.

HTTP

HTTP (Hypertext Transfer Protocol) est un protocole standard utilisé pour transférer des pages Web (y compris des graphiques et contenus multimédia) d'un serveur vers un client via Internet.

HTTPS

Protocole HTTP utilisant Secure Socket Layer (SSL). HTTPS est une variante de HTTP utilisée pour traiter les transactions sécurisées.

ICMP

Il arrive qu'une passerelle ou un hôte de destination utilise le protocole ICMP (Internet Control Message Protocol) pour communiquer avec un hôte source afin d'indiquer une erreur dans le traitement des datagrammes, par exemple. Le protocole ICMP utilise le support de base du protocole IP comme s'il s'agissait d'un protocole de niveau plus élevé ; cependant, le protocole ICMP fait en réalité partie intégrante du protocole IP et est implémenté par chaque module IP. Les messages ICMP sont envoyés dans les cas suivants : par exemple, lorsqu'un datagramme ne parvient pas à atteindre sa destination, lorsque la passerelle ne possède pas la capacité de tampon de transfert d'un datagramme et lorsque la passerelle peut diriger l'hôte afin d'acheminer le trafic via une route plus courte. Le protocole IP n'est pas conçu pour être parfaitement fiable. Le but de ces messages de contrôle est d'obtenir un retour d'informations concernant les problèmes dans l'environnement de communication, et non de rendre le protocole IP fiable.

IntelliScan

IntelliScan est une méthode d'identification des fichiers à scanner. Pour les fichiers exécutables (par exemple `.exe`), le véritable type du fichier est déterminé en fonction de

son contenu. Pour les fichiers non exécutables (au format `.txt` par exemple), le véritable type du fichier est déterminé en fonction de son en-tête.

IntelliScan offre les avantages suivants :

- Optimisation des performances : IntelliScan n'affecte pas les applications de l'agent, car il exploite une quantité minimale des ressources système.
- Durée de scan réduite : Comme IntelliScan est capable d'identifier le type réel des fichiers, il ne scanne que les fichiers réellement vulnérables aux infections. La durée du scan s'en trouve considérablement réduite, puisque tous les fichiers ne sont pas concernés.

IntelliTrap

Les auteurs de virus tentent souvent de contourner le filtrage antivirus en utilisant des algorithmes de compression en temps réel. IntelliTrap contribue à réduire les risques de telles incursions de virus sur le réseau en bloquant les fichiers exécutables compressés en temps réel et en les associant aux caractéristiques d'autres programmes malveillants. Étant donné qu'IntelliTrap identifie ces fichiers comme des risques de sécurité et peut bloquer malencontreusement des fichiers légitimes, Trend Micro vous recommande de mettre en quarantaine les fichiers (au lieu de les supprimer ou de les nettoyer) lorsque vous activez IntelliTrap. Si les utilisateurs échangent régulièrement des fichiers exécutables compressés en temps réel, désactivez IntelliTrap.

IntelliTrap utilise les composants suivants :

- Moteur de scan antivirus
- Signatures IntelliTrap
- Signatures d'exceptions IntelliTrap

IP

«Le protocole Internet (IP) permet de transmettre des blocs de données appelés datagrammes depuis l'emplacement source vers l'emplacement de destination, ces deux

emplacements étant des hôtes identifiés par des adresses de longueur définie.» (RFC 791)

Fichier Java

Java est un langage de programmation à usage général développé par Sun Microsystems. Un fichier Java contient du code Java. Java prend en charge la programmation sur Internet sous forme d'«applets» Java indépendantes des plates-formes. Une applet est un programme écrit en langage de programmation Java qui peut être inclus dans une page HTML. Lorsque vous utilisez un navigateur sur lequel la technologie Java est activée pour afficher une page contenant une applet, cette dernière transfère son code sur votre endpoint et la machine virtuelle Java du navigateur l'exécute.

LDAP

LDAP (Lightweight Directory Access Protocol) est un protocole applicatif permettant d'interroger et de modifier les services d'annuaire qui s'exécutent sur TCP/IP.

Port d'écoute

Un port d'écoute est utilisé pour les demandes de connexion des agents en vue d'un échange de données.

Agent MCP

Trend Micro Management Communication Protocol (MCP) constitue l'agent de nouvelle génération de Trend Micro pour les produits gérés. MCP remplace Trend Micro Management Infrastructure (TMI) comme moyen de communication entre Control Manager et OfficeScan. MCP introduit plusieurs nouvelles fonctions :

- Chargement du réseau et taille de paquets réduits

- Prise en charge de la traversée des NAT et des pare-feux
- Prise en charge de HTTPS
- Prise en charge des communications bilatérale et unilatérale
- Prise en charge de l'authentification unique (Single sign-on ou SSO)
- Prise en charge des nœuds de cluster

Menaces combinées

Les menaces combinées tirent profit de plusieurs points d'accès et vulnérabilités dans les réseaux d'entreprise (menaces « Nimda » ou « Code Red », par exemple).

NAT

NAT (Network Address Translation) est une norme permettant de traduire les adresses IP sécurisées en adresses temporaires externes enregistrées provenant du pool d'adresses. Cette norme permet aux réseaux de confiance utilisant des adresses IP affectées de manière privée d'accéder à Internet. Cela évite également de devoir obtenir une adresse IP enregistrée pour chaque ordinateur du réseau.

NetBIOS

NetBIOS (Network Basic Input Output System) est une interface de programmation d'application (API) qui apporte des fonctionnalités, notamment en matière de réseau, au système BIOS (Basic Input/Output System) du DOS (Disk Operating System).

Communication unilatérale

La traversée des NAT est devenue un problème de plus en plus sérieux dans les environnements réseau actuels. Pour résoudre ce problème, le protocole MCP utilise

une communication unilatérale. La communication unilatérale fait en sorte que l'agent MCP lance la connexion vers le serveur et teste les commandes provenant du serveur. Chaque requête correspond à une demande de commande de type CGI ou à une transmission de journal. Pour réduire l'impact sur le réseau, l'agent MCP maintient la connexion autant que possible. Toute demande ultérieure utilise une connexion déjà ouverte. Si la connexion est interrompue, toutes les connexions SSL au même hôte bénéficient d'un cache d'ID de session réduisant de manière significative le temps de reconnexion.

Patch

Un patch désigne un groupe de hot fixes et de correctifs de sécurité qui résolvent plusieurs problèmes du programme. Trend Micro publie régulièrement des patchs. Les patchs Windows comprennent un programme d'installation alors que les patchs non issus de Windows disposent en général d'un script d'installation.

Attaque de phishing

Le phishing est une forme de fraude se développant rapidement qui vise à duper les internautes en reproduisant à l'identique l'apparence de sites Web légitimes afin de divulguer des informations personnelles.

On rencontre généralement le cas suivant : un utilisateur non averti reçoit un e-mail manifestement urgent (et ayant l'air authentique) lui notifiant un problème relatif à son compte qu’il doit résoudre immédiatement sous peine de fermeture du compte. Cet e-mail inclut une adresse URL dirigeant vers un site Web qui a tous les aspects du site original. Il est facile de copier l'e-mail et le site Web légitimes, puis de modifier le serveur principal où sont collectées les données envoyées.

Le message invite l’utilisateur à se connecter au site et à confirmer des informations sur le compte. Un pirate reçoit les données fournies par l'utilisateur, par exemple, un identifiant, un mot de passe, un numéro de carte de crédit ou de sécurité sociale.

Ce genre de fraude est rapide, peu onéreux et simple d’exécution. C’est une méthode également relativement rentable pour les criminels qui la pratiquent. Le phishing est

difficile à détecter même pour les utilisateurs avertis. Il en est de même pour les autorités judiciaires. Pire encore, il est quasiment impossible de poursuivre ses auteurs en justice.

Veuillez signaler à Trend Micro tout site Web susceptible de pratiquer des activités de phishing.

Ping

Ping est un utilitaire qui envoie une requête d'écho ICMP à une adresse IP, puis attend la réponse. L'utilitaire Ping peut déterminer si le endpoint portant l'adresse IP spécifiée est en ligne ou non.

POP3

POP3 (Post Office Protocol 3) est un protocole standard pour le stockage et le transfert des messages depuis un serveur vers une application cliente de courrier électronique.

Serveur proxy

Un serveur proxy est un serveur Web acceptant les URL associées à un préfixe spécial, qui sert à extraire des documents d'une mémoire cache locale ou d'un serveur distant, puis renvoie l'URL au demandeur.

RPC

RPC (Remote Procedure Call) est un protocole réseau qui permet à un programme s'exécutant sur un hôte de lancer l'exécution de code sur un autre hôte.

Correctif de sécurité

Un Patch de sécurité est centré sur les problèmes de sécurité pouvant être déployés sur tous les clients. Les patchs de sécurité Windows comprennent un programme

d'installation alors que ceux qui ne sont pas issus de Windows disposent en général d'un script d'installation.

Service Pack

Un Service Pack désigne un regroupement de hot fixes, de correctifs et d'améliorations de fonctions suffisamment significatives pour être considérées comme une mise à niveau du produit. Les service packs Windows et non-Windows contiennent un programme et un script d'installation.

SMTP

SMTP (Simple Mail Transport Protocol) est un protocole standard utilisé pour acheminer les messages électroniques d'un serveur vers un autre et d'un agent vers un serveur, via Internet.

SNMP

SNMP (Simple Network Management Protocol) est un protocole qui permet de surveiller les dispositifs connectés à un réseau afin de détecter les situations nécessitant une intervention de l'administrateur.

Déroutement SNMP

Un déroutement SNMP (Simple Network Management Protocol, protocole simple de gestion de réseau) est un procédé d'envoi de notifications aux administrateurs réseau qui utilisent des consoles d'administration prenant en charge ce protocole.

OfficeScan peut stocker les notifications dans les MIB (Management Information Bases ou bases d'informations d'administration). Vous pouvez utiliser les navigateurs MIB pour visualiser les notifications par déroutement SNMP.

SOCKS°4

SOCKS 4 est un protocole TCP utilisé par les serveurs proxy pour établir une connexion entre les agents du réseau interne ou LAN et les endpoints ou serveurs externes au LAN. Le protocole SOCKS°4 soumet des demandes de connexion, établit des circuits proxy et relaie les données au niveau de la couche application du modèle OSI.

SSL

Protocole conçu par Netscape pour assurer la sécurité des données, constituant une couche entre les protocoles d'application (tels que HTTP, Telnet ou FTP) et TCP/IP. Ce protocole de sécurité assure le chiffrement des données, l'authentification du serveur, l'intégrité des messages et l'authentification éventuelle des agents pour une connexion TCP/IP.

Certificat SSL

Ce certificat numérique crée une communication HTTPS sécurisée.

TCP

TCP (Transmission Control Protocol) est un protocole de bout en bout fiable et orienté connexion conçu pour s'adapter à une hiérarchie de protocoles en couches prenant en charge des applications multiréseau. Le protocole TCP dépend des datagrammes IP pour la résolution des adresses. Consultez DARPA Internet Program RFC 793 pour de plus amples informations.

Telnet

Il s'agit d'une méthode standard de liaison entre des dispositifs terminaux via le protocole TCP grâce à la création d'un «terminal virtuel de réseau». Consultez Network Working Group RFC 854 pour de plus amples informations.

Port des chevaux de Troie

Les ports des chevaux de Troie sont couramment utilisés par les programmes de type cheval de Troie pour se connecter à un endpoint. Lors d'une épidémie, OfficeScan bloque les numéros de port suivants, susceptibles d'être utilisés par des chevaux de Troie.

Tableau E-1. Ports des chevaux de Troie

Numéro de port	Cheval de Troie	Numéro de port	Cheval de Troie
23432	Asylum	31338	Net Spy
31337	Back Orifice	31339	Net Spy
18006	Back Orifice 2000	139	Nuker
12349	Bionet	44444	Prosiak
6667	Bionet	8012	Ptakks
80	Codered	7597	Qaz
21	DarkFTP	4000	RA
3150	Deep Throat	666	Ripper
2140	Deep Throat	1026	RSM
10048	Delf	64666	RSM
23	EliteWrap	22222	Rux
6969	GateCrash	11000	Senna Spy

Numéro de port	Cheval de Troie	Numéro de port	Cheval de Troie
7626	Gdoor	113	Shiver
10100	Gift	1001	Silencer
21544	Girl Friend	3131	SubSari
7777	GodMsg	1243	Sub Seven
6267	GW Girl	6711	Sub Seven
25	Jesrto	6776	Sub Seven
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	Net Bus	12345	Valvo line
7300	Net Spy	1234	Valvo line

Port sécurisé

Le serveur et l'agent OfficeScan utilisent des ports sécurisés pour communiquer entre eux.

Si vous bloquez les ports sécurisés, puis restaurez les paramètres réseau habituels après une épidémie, les agents OfficeScan ne rétabliront pas immédiatement la communication avec le serveur. La communication agent-serveur ne sera rétablie qu'après écoulement du nombre d'heures que vous avez indiqué sur l'écran Paramètres de prévention des épidémies.

OfficeScan utilise le port HTTP (par défaut, 8080) comme port sécurisé sur le serveur. Lors de l'installation, il vous est possible de saisir un numéro de port différent. Pour bloquer ce port sécurisé ainsi que le port sécurisé sur l'agent OfficeScan, vous devez cocher la case Bloquer les ports sécurisés sur l'écran Blocage de ports.

Le programme d'installation principal génère de façon aléatoire le port sécurisé de l'agent OfficeScan pendant l'installation.

Détermination des ports sécurisés

Procédure

1. Accédez au répertoire <*dossier d'installation du serveur*>`\PCCSRV`.
2. Ouvrez le fichier `ofcscan.ini` à l'aide d'un éditeur de texte comme le Bloc-notes.
3. Pour définir le port sécurisé du serveur, recherchez la chaîne «Master_DomainPort» et vérifiez la valeur figurant en regard de celle-ci.

   Par exemple, si la chaîne est la suivante : `Master_DomainPort=80`, cela signifie que le port 80 constitue le port sécurisé sur le serveur.
4. Pour définir le port sécurisé de l'agent, recherchez la chaîne « Client_LocalServer_Port » et vérifiez la valeur figurant en regard de celle-ci.

   Par exemple, si la chaîne est la suivante : `Client_LocalServer_Port=41375`, cela signifie que le port 41375 constitue le port sécurisé sur l'agent.

Communication bilatérale

La communication bilatérale constitue une alternative à la communication unilatérale. Basée sur la communication unilatérale, mais disposant d'un canal HTTP supplémentaire recevant des notifications du serveur, la communication bilatérale permet d'améliorer l'envoi en temps réel et le traitement des commandes depuis le serveur par l'agent MCP.

UDP

UDP (User Datagram Protocol) est un protocole de communication sans connexion utilisé avec le protocole IP pour permettre aux programmes d'application d'envoyer des messages à d'autres programmes. Consultez DARPA Internet Program RFC 768 pour de plus amples informations.

Fichiers non nettoyables

Le moteur de scan antivirus ne nettoie pas les fichiers suivants :

Tableau E-2. Solutions aux problèmes de fichiers non nettoyables

Fichier non nettoyable	Explication et solution
Fichiers infectés par des chevaux de Troie	Les chevaux de Troie sont des programmes qui exécutent des actions inattendues, non autorisées et généralement nuisibles, telles que l'affichage de messages, l'écrasement de fichiers ou le formatage de disques. Il est inutile de nettoyer les fichiers puisque les chevaux de Troie ne les infectent pas. Solution : le moteur de nettoyage de virus et le modèle de nettoyage de virus suppriment les chevaux de Troie.
Fichiers infectés par des vers	Un ver informatique est un programme (ou ensemble de programmes) autonome qui peut répandre des copies fonctionnelles de lui-même ou de ses segments au sein d'autres systèmes informatiques. La propagation se produit généralement par le biais de connexions réseau ou de pièces jointes d'e-mails. Les vers ne peuvent pas être nettoyés car le fichier constitue un programme autonome. Solution : Trend Micro recommande de supprimer les vers.
Fichiers infectés protégés en écriture	Solution : supprimez la protection en écriture pour permettre le nettoyage du fichier.
Fichiers protégés par mot de passe	Les fichiers protégés par mot de passe sont notamment les fichiers compressés protégés par mot de passe ou les fichiers Microsoft Office protégés par mot de passe. Solution : supprimez la protection par mot de passe pour permettre le nettoyage du fichier.

FICHIER NON NETTOYABLE	EXPLICATION ET SOLUTION
Fichiers de sauvegarde	Les fichiers possédant une extension RB0~RB9 sont des copies de sauvegarde des fichiers infectés. Le processus de nettoyage crée une sauvegarde du fichier infecté au cas où le virus/ programme malveillant l'endommagerait. Solution : si le fichier infecté a pu être nettoyé, il est inutile de conserver la copie de sauvegarde. Si le endpoint fonctionne correctement, vous pouvez supprimer le fichier de sauvegarde.

FICHIER NON NETTOYABLE	EXPLICATION ET SOLUTION
Fichiers infectés dans la corbeille	Le système, s'il est en cours d'exécution, peut refuser la suppression des fichiers infectés placés dans la Corbeille.

	Solution pour Windows XP ou Windows Server 2003 avec système de fichiers NTFS :
	1. Connectez-vous au endpoint avec des privilèges d'administrateur.
	2. Fermez toutes les applications en cours afin d'éviter que celles-ci ne verrouillent le fichier, empêchant ainsi Windows de le supprimer.
	3. Ouvrez une invite de commandes.
	4. Saisissez ce qui suit pour effacer les fichiers :
	`cd \`
	`cd recycled`
	`del *.* /S`
	La dernière commande supprime tous les fichiers de la corbeille.
	5. Vérifiez si les fichiers ont été supprimés.

	Solution pour les autres systèmes d'exploitation (ou ceux sans NTFS) :
	1. Redémarrez le endpoint en mode MS-DOS.
	2. Ouvrez une invite de commandes.
	3. Saisissez ce qui suit pour effacer les fichiers :
	`cd \`
	`cd recycled`
	`del *.* /S`
	La dernière commande supprime tous les fichiers de la corbeille.

Fichier non nettoyable	Explication et solution
Fichiers infectés dans le dossier Temp de Windows ou dans un dossier temporaire d'Internet Explorer	Il est possible que le système refuse le nettoyage des fichiers infectés se trouvant dans le dossier Temp de Windows ou dans le dossier temporaire d'Internet Explorer car le endpoint les utilise. Les fichiers à nettoyer sont peut-être des fichiers temporaires nécessaires au fonctionnement de Windows.

Fichier non nettoyable	Explication et solution

	Solution pour Windows XP ou Windows Server 2003 avec système de fichiers NTFS :
	1. Connectez-vous au endpoint avec des privilèges d'administrateur.
	2. Fermez toutes les applications en cours afin d'éviter que celles-ci ne verrouillent le fichier, empêchant ainsi Windows de le supprimer.
	3. Si le fichier infecté se trouve dans le dossier Temp de Windows:
	a. Ouvrez l'invite de commandes et remplacez le répertoire existant par le répertoire Temp de Windows (situé par défaut sous `C:\Windows\Temp` sur les endpoints Windows XP ou Windows Server 2003).
	b. Saisissez ce qui suit pour effacer les fichiers :
	`cd temp`
	`attrib -h`
	`del *.* /S`
	La dernière commande supprime tous les fichiers du dossier Temp de Windows.
	4. Si le fichier infecté se trouve dans le dossier temporaire d'Internet Explorer:
	a. Ouvrez une invite de commandes et accédez au dossier temporaire d'Internet Explorer (situé par défaut sous `C:\Documents and Settings\<Votre nom d'utilisateur>\Local Settings\Temporary Internet Files` pour les endpoints fonctionnant sous Windows XP ou Server 2003).
	b. Saisissez ce qui suit pour effacer les fichiers :
	`cd tempor~1`
	`attrib -h`
	`del *.* /S`
	La dernière commande supprime tous les fichiers du dossier temporaire d'Internet Explorer.
	c. Vérifiez si les fichiers ont été supprimés.

Fichier non nettoyable	Explication et solution
	Solution pour les autres systèmes d'exploitation (ou ceux sans NTFS) : 1. Redémarrez le endpoint en mode MS-DOS. 2. Si le fichier infecté se trouve dans le dossier Temp de Windows: a. Ouvrez l'invite de commandes et remplacez le répertoire existant par le répertoire Temp de Windows (situé par défaut sous C:\Windows\Temp sur les endpoints Windows XP ou Windows Server 2003). b. Saisissez ce qui suit pour effacer les fichiers : cd temp attrib -h del *.* /S La dernière commande supprime tous les fichiers du dossier Temp de Windows. c. Redémarrez le endpoint en mode normal. 3. Si le fichier infecté se trouve dans le dossier temporaire d'Internet Explorer: a. Ouvrez une invite de commandes et accédez au dossier temporaire d'Internet Explorer (situé par défaut sous C:\Documents and Settings\<Votre nom d'utilisateur>\Local Settings\Temporary Internet Files pour les endpoints fonctionnant sous Windows XP ou Server 2003). b. Saisissez ce qui suit pour effacer les fichiers : cd tempor~1 attrib -h del *.* /S La dernière commande supprime tous les fichiers du dossier temporaire d'Internet Explorer. c. Redémarrez le endpoint en mode normal.

Fichier non nettoyable	Explication et solution
Fichiers compressés à l'aide d'un format de compression non pris en charge	Solution : décompressez les fichiers.
Fichiers verrouillés ou en cours d'exécution	Solution : déverrouillez les fichiers ou attendez que l'exécution de ces fichiers soit terminée.
Fichiers corrompus	Solution : supprimez les fichiers.

Fichiers infectés par des chevaux de Troie

Les chevaux de Troie sont des programmes qui exécutent des actions inattendues, non autorisées et généralement nuisibles, telles que l'affichage de messages, l'écrasement de fichiers ou le formatage de disques. Il est inutile de nettoyer les fichiers puisque les chevaux de Troie ne les infectent pas.

Solution : OfficeScan utilise le moteur de nettoyage de virus et le modèle de nettoyage de virus pour supprimer les chevaux de Troie.

Fichiers infectés par des vers

Un ver informatique est un programme (ou ensemble de programmes) autonome qui peut répandre des copies fonctionnelles de lui-même ou de ses segments au sein d'autres systèmes informatiques. La propagation se produit généralement par le biais de connexions réseau ou de pièces jointes d'e-mails. Les vers ne peuvent pas être nettoyés car le fichier constitue un programme autonome.

Solution : Trend Micro recommande de supprimer les vers.

Fichiers infectés protégés en écriture

Solution : supprimez la protection en écriture pour autoriser OfficeScan à nettoyer le fichier.

Fichiers protégés par mot de passe

Comprennent les fichiers compressés protégés par mot de passe et les fichiers Microsoft Office protégés par mot de passe.

Solution : supprimez la protection par mot de passe pour qu'OfficeScan puisse nettoyer ces fichiers.

Fichiers de sauvegarde

Les fichiers possédant une extension RB0~RB9 sont des copies de sauvegarde des fichiers infectés. OfficeScan crée une sauvegarde du fichier infecté au cas où le virus/ programme malveillant l'endommagerait au cours du processus de nettoyage.

Solution : si OfficeScan a réussi à nettoyer le fichier infecté, vous n'avez pas besoin de conserver la copie de sauvegarde. Si le endpoint fonctionne correctement, vous pouvez supprimer le fichier de sauvegarde.



Index

B

C

N

O

R

S

T